NetScreen-RA 500

Administrationshandbuch

NetScreen Instant Virtual Extranet Platform

Juniper Networks NetScreen Secure Access 700

Administration

Version 5.1

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Teilenummer: 42A112204

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, Neoteris, Neoteris-Secure Access, Neoteris-Secure Meeting, NetScreen-SA 1000, NetScreen-SA 3000, NetScreen-SA 5000, IVE, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetsukeTeilenummer: 42A112204en-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Copyright © 2001 D. J. Bernstein. Copyright © 1985-2003 by the Massachusetts Institute of Technology. All rights reserved. Copyright © 2000 by Zero-Knowledge Systems, Inc. Copyright © 2001, Dr. Brian Gladman <brg@gladman.uk.net>, Worcester, UK. All rights reserved. Copyright © 1989, 1991 Free Software Foundation, Inc. Copyright © 1989, 1991, 1992 by Carnegie Mellon University. Derivative Work - 1996, 1998-2000. Copyright © 1996, 1998-2000 The Regents of the University of California. All Rights Reserved. Copyright © 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted. Copyright © 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland. All rights reserved. Copyright © 1986 Gary S. Brown. Copyright © 1998 CORE SDI S.A., Buenos Aires, Argentina. Copyright © 1995, 1996 by David Mazieres <dm@lcs.mit.edu>. Copyright © 1998-2002. The OpenSSL Project. All rights reserved. Copyright © 1989-2001, Larry Wall. All rights reserved. Copyright © 1989, 1991 Free Software Foundation, Inc. Copyright © 1996-2002 Andy Wardley. All Rights Reserved. Copyright © 1998-2002. Canon Research Centre Europe Ltd. Copyright © 1995-1998. Jean-loup Gailly and Mark Adler.

Juniper Networks NetScreen Secure Access 700, Release 5.1

Copyright © 2005, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writers:

Editors:

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Inhalt

Das Handbuch ix

Teil 1 **Erste Schritte** 1

Kapitel 1 **Erste Überprüfung und Schlüsselkonzepte** 3

Überprüfen der Verfügbarkeit für die Benutzer 5
Anlegen eines Testszenarios, um die Grundlagen und empfohlenen Vorgehensweisen für das **IVE** kennen zu lernen 8
Definieren einer Benutzerrolle 8
Definieren einer Ressourcenrichtlinie 11
Definieren eines Authentifizierungsservers 14
Definieren eines Authentifizierungsbereichs 17
Definieren einer Anmelderichtlinie 20
Verwenden des Testszenarios 23
Standardeinstellungen für Administratoren 26

Teil 2 **IVE Produkte und Funktionen** 29

Kapitel 2 **Die IVE-Reihe** 31

Einführung in die NetScreen Instant Virtual Extranet-Plattform 33
Was ist die IVE-Plattform? 33
Wie bauen Produkte auf der Funktionsweise der IVE-Plattform auf? 34
Access Series – Übersicht 37
Zugriffsverwaltung – Übersicht 38
Richtlinien, Regeln und Einschränkungen sowie Bedingungen 38
Zugriff und Autorisierung – Flussdiagramm 40
Dynamic Policy Evaluation (Dynamische Richtlinienauswertung) 44
Konfigurieren von Sicherheitsanforderungen 46
Authentifizierungsbereiche – Übersicht 51
Authentifizierungsserver 51
Authentifizierungsrichtlinien 53
Verzeichnisserver 53
Rollenzuordnungsregeln 53
Anmelderichtlinien – Übersicht 55
Anmeldeseiten 55
Benutzerrollen – Übersicht 56
Rollenarten 56
Rollenkomponenten 56
Rollenauswertung 57

Ressourcenrichtlinien – Übersicht 59
Typen von Ressourcenrichtlinien 59
Bestandteile einer Ressourcenrichtlinie 59
Auswerten von Ressourcenrichtlinien 60
Ausführliche Regeln für Ressourcenrichtlinien 60

Kapitel 3 Authentifizierung und Autorisierung 63

Zertifikate – Übersicht 65
IVE Serverzertifikate 66
CAs vertrauter Clients 67
CAs vertrauter Server 71
Codesignaturzertifikate 72
Endpoint Defense – Übersicht 74
Host Checker – Übersicht 75
Cache Cleaner – Übersicht 87

Kapitel 4 Remotezugriff 93

Network Connect – Übersicht 95
Automatische Network Connect-Anmeldung mit „GINA“ 98
Bereitstellen Ihres Netzwerks für Network Connect 100
Definieren von Zugriffsmethoden mit Hilfe von Network Connect-Ressourcenrichtlinien 101
Clientseitige Protokollierung 102
Network Connect Proxy-Unterstützung 103
E-Mail-Client – Übersicht 106
Auswählen eines E-Mail-Clients 106
Arbeiten mit einem standardbasierten Mailserver 107
Arbeiten mit Microsoft Exchange Server 108
Arbeiten mit Lotus Notes und Lotus Notes Mail Server 110
Hochladen eines Java-Applets - Übersicht 111
Hochladen von Java-Applets in das IVE 111
Signieren von hochgeladenen Java-Applets 112
Erstellen von HTML-Seiten, die auf die hochgeladenen Java-Applets verweisen 113
Zugreifen auf Lesezeichen für Java-Applets 113
Verwendungsbeispiel: Erstellen eines Lesezeichens für ein Java-Applet mit Citrix JICA Version 8.0 114
Durchgangsproxy – Übersicht 117

Kapitel 5 Systemverwaltung und Systemdienste 121

Netzwerkeinstellungen – Übersicht 123
Konfigurieren allgemeiner Netzwerkeinstellungen 123
Konfigurieren interner und externer Ports 123
Konfigurieren von statischen Routen für den Netzwerkverkehr 124
Erstellen von ARP-Zwischenspeichern 124
Angeben von Hostnamen zur lokalen Auflösung durch das IVE 125
Angeben von IP-Filtern 125
Protokollierung und Überwachung – Übersicht 126
Konfigurationsdateien – Übersicht 129
Archivieren von IVE-Konfigurationsdateien 129
Importieren und Exportieren von IVE-Konfigurationsdateien 130
Importieren und Exportieren von XML-Konfigurationsdateien 130
Strategien für die Arbeit mit XML-Instanzen 142

Fehlerbehebung – Übersicht 144
Simulieren oder Verfolgen von Ereignissen 144
Erstellen von Snapshots des IVE-Systemstatus 145
Erstellen von TCP-Dumpdateien 145
Testen der IVE-Netzwerkverbindung 146
Remoteausführung von Debuggingtools 147
Erstellen von Debuggingprotokollen 147
Unterstützung mehrerer Sprachen – Übersicht 148

Teil 3 **IVE Konfiguration** **149**

Aufgabenzusammenfassungen **151**

Kapitel 6 **Systemeinstellungen** **153**

Konfigurieren der Seite „Status“ 155
Registerkarte „Overview“ 155
Registerkarte „Active Users“ 156
Konfigurieren der Seite „Configuration“ 158
Registerkarte „Licensing“ 158
Seite „Security“ 164
Registerkarten „Certificates“ 166
Registerkarte „NCP“ 182
Registerkarte „Client Types“ 183
Konfigurieren der Seite „Network“ 186
Registerkarte „Overview“ 186
Registerkarten „Internal Port“ 187
Registerkarten „External Port“ 188
Registerkarte „Routes“ 189
Registerkarte „Hosts“ 190
Registerkarte „Network Connect“ 190
Konfigurieren der Seite „Log Monitoring“ 191
Registerkarten „Events“, „User Access“ „Admin Access“ und „NC Packet“ 191
Registerkarte „SNMP“ 193
Registerkarte „Statistics“ 199
Registerkarte „Client-side Logs“ 199

Kapitel 7 **Anmeldeeinstellungen** **201**

Konfigurieren der Seite „Sign-in“ 203
Registerkarte „Sign-in Policies“ 203
Registerkarte „Sign-in Pages“ 204
Konfigurieren der Seite „End Point“ 206
Registerkarte „Host Checker“ 206
Registerkarte „Cache Cleaner“ 220
Konfigurieren der Seite „AAA Servers“ 223
Definieren einer Authentifizierungsserverinstanz 224
Ändern einer Authentifizierungsserverinstanz 224
Konfigurieren einer lokalen Authentifizierungsserverinstanz 225
Konfigurieren einer LDAP-Serverinstanz 230
Konfigurieren einer NIS-Serverinstanz 233
Konfigurieren einer ACE/Serverinstanz 234

Konfigurieren einer RADIUS-Serverinstanz 238
Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz .. 245
Konfigurieren einer Instanz eines anonymen Servers 250
Konfigurieren einer Zertifikatserverinstanz 252
Anzeigen und Löschen von Benutzersitzungen 254

Kapitel 8 Administratoreinstellungen 255

Konfigurieren der Seite „Authentication“ 257
Registerkarte „General“ 257
Registerkarte „Authentication Policy“ 259
Registerkarte „Role Mapping“ 260
Konfigurieren der Seite „Delegation“ 267
Konfigurieren von Administratorrollen 267
Registerkarten „General“ 267

Kapitel 9 Benutzereinstellungen 273

Konfigurieren der Seite „Authentication“ 275
Konfigurieren der Seite „Roles“ 276
Konfigurieren der Seite „General“ 277
Registerkarte „Overview“ 277
Registerkarte „Restrictions“ 278
Registerkarte „Source IP“ 278
Registerkarte „Session Options“ 279
Registerkarte „UI Options“ 281
Konfigurieren der Seite „Web“ 284
Registerkarte „Bookmarks“ 284
Registerkarte „Options“ 287
Konfigurieren der Seite „Files“ 292
Registerkarte „Web Bookmarks“ 292
Registerkarte „UNIX Bookmarks“ 293
Registerkarte „Options“ 294
Konfigurieren der Seite „Telnet/SSH“ 296
Registerkarte „Sessions“ 296
Registerkarte „Options“ 297
Konfigurieren der Seite „Network Connect“ 299
Konfigurieren der Seite „New User“ 301

Kapitel 10 Ressourcenrichtlinieneinstellungen 303

Angeben von Ressourcen für eine Ressourcenrichtlinie 305
Allgemeine Anmerkungen zu kanonischen Formaten 305
Angeben von Serverressourcen 305
Schreiben einer detaillierten Regel 306
Konfigurieren der Seite „Web“ 308
Registerkarte „Access“ 311
Registerkarten „Caching“ 312
Registerkarten „Java“ 316
Registerkarten „Rewriting“ 320
Registerkarten „Web Proxy“ 328
Registerkarte „Compression“ 330
Registerkarte „Options“ 331
Konfigurieren der Seite „Files“ 332
Windows-Registerkarten 334
Registerkarte „UNIX/NFS“ 337

Registerkarte „Compression“ 338
Registerkarte „Encoding“ 339
Registerkarte „Options“ 340
Konfigurieren der Seite „Telnet/SSH“ 341
Registerkarte „Access“ 341
Registerkarte „Options“ 343
Konfigurieren der Seite „Network Connect“ 344
Registerkarte „Network Connect Access Control“ 344
Registerkarte „Network Connect Logging“ 345
Registerkarte „Network Connect Connection Profiles“ 346
Registerkarte „Network Connect Split Tunneling“ 350
Verwendungsbeispiel: Konfiguration von Network Connect-Ressourcenrichtlinien 352
Konfigurieren der Seite „Email Client“ 354

Kapitel 11 Wartungseinstellungen 357

Konfigurieren der Seite „System“ 359
Registerkarte „Platform“ 359
Registerkarte „Upgrade/Downgrade“ 360
Registerkarte „Options“ 361
Registerkarte „Installers“ 361
Konfigurieren der Seite „Import/Export“ 364
Registerkarte „Configuration“ 364
Registerkarte „User Accounts“ 365
Registerkarte „XML Import/Export“ 366
XML Import/Export – Gebrauchsfälle 370
Konfigurieren der Seite „Archiving“ 376
Registerkarte „FTP Server“ 376
Konfigurieren der Seite „Troubleshooting“ 378
„User Sessions“-Registerkarten 378
Registerkarte „Session Recording“ 381
Registerkarte „System Snapshot“ 382
Registerkarte „TCP Dump“ 382
Registerkarte „Commands“ 383
Registerkarte „Remote Debugging“ 384
Registerkarte „Debug Log“ 385

Teil 4 Zusatzinformationen 387

Anhang A Verwenden der seriellen Konsole der IVE-Appliance 389

Herstellen einer Verbindung mit der seriellen Konsole der IVE-Appliance 389
Rollback zu einem vorherigen Systemzustand 390
Zurücksetzen einer IVE-Appliance auf die Werkseinstellungen 392
Durchführen gängiger Wiederherstellungsvorgänge 395

Anhang B Schreiben benutzerdefinierter Ausdrücke 397

Benutzerdefinierte Ausdrücke 397
Systemvariablen und Beispiele 401

Anhang C Installation von clientseitigen Anwendungen 411

Erforderliche Berechtigungen zum Installieren und Ausführen von Anwendungen 411
Anwendungsdateiverzeichnisse 412

Anhang D Konfigurieren der Zugriffsverwaltungsbeschränkungen 417

IP-Quelladresseinschränkungen 417
Browsereinschränkungen 419
Zertifikateinschränkungen 421
Kennworteinschränkung 422
Host Checker-Einschränkungen 423
Cache Cleaner-Einschränkungen 424

Anhang E Benutzerfehlermeldungen 427

Fehlermeldungen in Network Connect 427
Windows-Fehlermeldungen 427
Macintosh-Fehlermeldungen 442
Index 451

Das Handbuch

In diesem Handbuch finden Sie die erforderlichen Informationen zum Konfigurieren und Verwalten der Secure Access 700-Appliance, unter anderem zu den folgenden Themen:

- Übersicht über die Secure Access 700-Appliance und das zugrunde liegende Zugriffsverwaltungssystem
- Übersicht über die Funktionen der Secure Access 700-Appliance
- Anweisungen für die Konfiguration und Verwaltung Ihrer Secure Access 700-Appliance

Zielgruppe

Dieses Handbuch wendet sich an Systemadministratoren, die für die Konfiguration von Secure Access 700-Appliances zuständig sind.

Weiterführende Informationen

Informationen zur Installation können Sie dem Leitfaden für die ersten Schritte entnehmen, der dem Produkt beiliegt. Den neuesten Build des Secure Access 700-Betriebssystems mit dem zugehörigen *Administratorhandbuch* im PDF-Format und den Versionshinweisen können Sie auf der Juniper Networks-Supportsite herunterladen.

Konventionen

Tabelle 1 definiert in diesem Handbuch verwendete Hinweissymbole, und Tabelle 2 erläutert die im Handbuch geltenden Textkonventionen.

Tabelle 1: Hinweissymbole

Symbol	Bedeutung	Beschreibung
	Informativer Hinweis	Weist auf wichtige Funktionen oder Anweisungen hin.
	Vorsicht	Weist auf die Möglichkeit von Datenverlusten oder Hardwarebeschädigung hin.
	Warnung	Weist auf Verletzungsgefahr hin.

Tabelle 2: Textkonventionen (gilt nicht für Befehlssyntax)

Konvention	Beschreibung	Beispiele
Fett	Wird für Schaltflächen, Feldnamen, Dialogfeldnamen und andere Benutzeroberflächenelemente verwendet.	Verwenden Sie zum Planen einer Konferenz die Registerkarten **Scheduling** und **Appointment**.
Plain Sans Serif	Stellt Folgendes dar: ■ Code, Befehle und Schlüsselwörter ■ URLs, Dateinamen und Verzeichnisse	Beispiele: ■ Code: certAttr.OU = 'Retail Products Group' ■ URL: Laden Sie die JRE-Anwendung unter folgender Adresse herunter: http://java.sun.com/j2se/
Kursiv	Stellt Folgendes dar: ■ Im Text definierte Begriffe ■ Variable Elemente ■ Buchnamen	Beispiele: ■ Definierter Begriff: Ein *RDP-Client* ist eine Windows-Komponente, die eine Verbindung zwischen einem Windows-Server und dem Computer eines Benutzers ermöglicht. ■ Variables Element : Verwenden Sie die Einstellungen auf der Seite **Users** > **Roles** > *Ausgewählte Rolle* > **Terminal Services**, um eine Terminalemulationssitzung zu erstellen. ■ Buchname: Siehe das Dokument *IVE Supported Platforms*.

Dokumentation

Versionshinweise

Versionshinweise sind in der Produktsoftware enthalten und im Internet verfügbar.

In den *Versionshinweisen* finden Sie aktuellste Informationen zu Funktionen, Änderungen, bekannten und gelösten Problemen. Wenn die Informationen in den *Versionshinweisen* von den Angaben in der Dokumentation abweichen, haben die *Versionshinweise* Vorrang.

Webzugriff

Auf der folgenden Seite können Sie die Dokumentation im Internet anzeigen:

http://www.juniper.net/techpubs/

Kundensupport

Wenn Sie technischen Support benötigen, wenden Sie sich unter support@juniper.net oder 1-888-314-JTAC (in den USA) oder 408-745-9500 (außerhalb der USA) an Juniper Networks.

Teil 1

Erste Schritte

In diesem Abschnitt werden zusätzliche IVE-Konfigurationsaufgaben beschrieben, mit deren Hilfe Sie sich mit den erforderlichen Konzepten für die Aktivierung und Steuerung des Benutzerzugriffs im Netzwerk vertraut machen können.

Inhalt

- „Erste Überprüfung und Schlüsselkonzepte“ auf Seite 3

Kapitel 1

Erste Überprüfung und Schlüsselkonzepte

In diesem Abschnitt werden die nach der Erstinstallation und -konfiguration des IVE durchzuführenden Aufgaben erläutert. Dieser Abschnitt setzt voraus, dass Sie die im Aufgabenhandbuch beschriebenen Schritte bereits auf der Administrator-Webkonsole ausgeführt haben, um Ihr Softwareabbild zu aktualisieren und Ihren Secure Access-Lizenzschlüssel zu generieren und anzuwenden.

Inhalt

- „Überprüfen der Verfügbarkeit für die Benutzer“ auf Seite 5
- „Anlegen eines Testszenarios, um die Grundlagen und empfohlenen Vorgehensweisen für das IVE kennen zu lernen“ auf Seite 8
- „Standardeinstellungen für Administratoren“ auf Seite 26

Überprüfen der Verfügbarkeit für die Benutzer

Sie können auf dem System-Authentifizierungsserver einfach ein Benutzerkonto anlegen, mit dem Sie die Verfügbarkeit des IVE für die Benutzer testen können. Legen Sie das Konto zunächst über die Administrator-Webkonsole an, und melden Sie sich dann auf der Benutzer-Anmeldeseite des IVE als dieser Benutzer an.

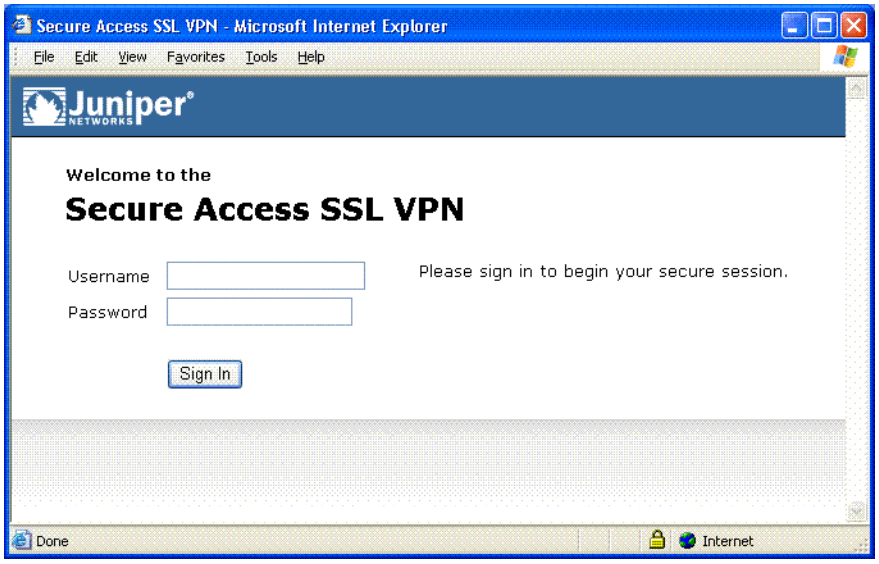
So überprüfen Sie die Verfügbarkeit für die Benutzer:

1. Wählen Sie in der Administrator-Webkonsole **Users > New User** aus.

2. Geben Sie auf der Seite **New Local User** „testbenutzer1“ als Benutzernamen und ein Kennwort ein, und klicken Sie dann auf **Save Changes**. Das IVE legt das Konto „testbenutzer1“ an.

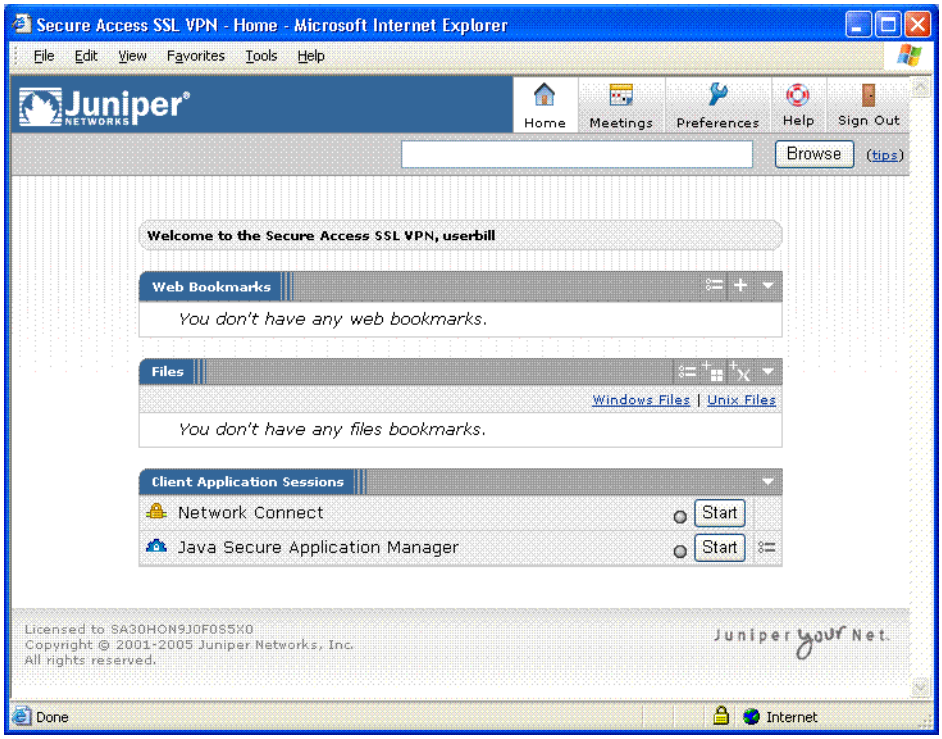
3. Geben Sie in einem anderen Browser den Geräte-URL ein, um zur Benutzer-Anmeldeseite zu navigieren. Der URL weist folgendes Format auf: `https://a.b.c.d/test`, wobei `a.b.c.d` die IP-Adresse des Geräts ist, die Sie während der Erstkonfiguration des IVE eingegeben haben. Wenn Sie in einer Sicherheitswarnung gefragt werden, ob Sie ohne signiertes Zertifikat fortfahren möchten, klicken Sie auf **Yes**. Wenn die Benutzer-Anmeldeseite angezeigt wird, haben Sie das IVE ordnungsgemäß mit dem Netzwerk verbunden.

Abbildung 1: Benutzer-Anmeldeseite



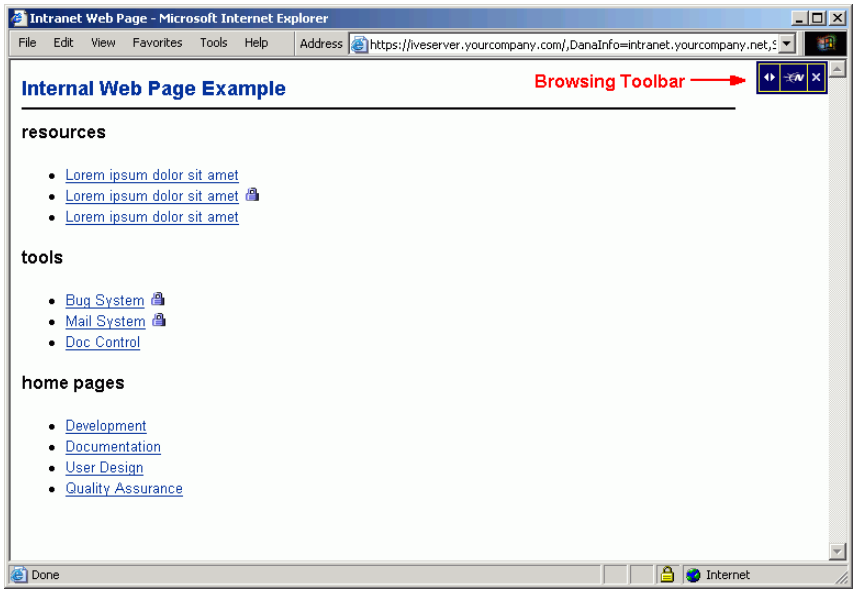
4. Geben Sie auf der Anmeldeseite die Anmeldeinformationen (Benutzername und Kennwort) ein, die Sie für das Benutzerkonto angelegt haben, und klicken Sie dann auf **Sign In**, um auf die IVE-Startseite für Benutzer zu gelangen.

Abbildung 2: Benutzerstartseite (Standard)



5. Geben Sie im Feld **Address** des Browsers den URL zu einem internen Webserver ein, und klicken Sie auf **Browse**. Das IVE öffnet die Webseite in demselben Browserfenster. Kehren Sie daher zur IVE-Startseite zurück, und klicken Sie auf der Navigationssymbolleiste, die auf der Zielwebseite angezeigt wird, auf das Symbol in der Mitte.

Abbildung 3: Beispiel für interne Webseite mit Navigationssymbolleiste



6. Geben Sie auf der IVE-Startseite den URL zur externen Firmensite ein, und klicken Sie auf **Wechseln zu**. Das IVE öffnet die Webseite in demselben Browserfenster. Kehren Sie daher über die Navigationssymbolleiste zur IVE-Startseite zurück.

7. Klicken Sie auf der IVE-Startseite auf **Browsing > Windows Files**, um zu verfügbaren Windows-Dateifreigaben zu navigieren, oder auf **Browsing > UNIX/NFS Files**, um zu verfügbaren UNIX/NFS-Dateifreigaben zu navigieren.

Nachdem Sie die Verfügbarkeit für die Benutzer überprüft haben, kehren Sie zur Administrator-Webkonsole zurück, um wie unter „Anlegen eines Testszenarios, um die Grundlagen und empfohlenen Vorgehensweisen für das IVE kennen zu lernen“ auf Seite 8 beschrieben an einer Einführung in die Schlüsselkonzepte teilzunehmen.

Anlegen eines Testszenarios, um die Grundlagen und empfohlenen Vorgehensweisen für das IVE kennen zu lernen

Das IVE bietet ein flexibles Zugriffsverwaltungssystem, mit dem der Remotezugriff eines Benutzers problemlos anhand von Rollen, Ressourcenrichtlinien, Authentifizierungsservern, Authentifizierungsbereichen und Anmelderichtlinien individuell angepasst werden kann. Damit Sie zügig mit diesen Elementen arbeiten können, sind für diese im IVE werksseitig bereits Standardvorgaben eingestellt. In diesem Abschnitt werden die Systemstandardvorgaben erläutert, und es wird dargestellt, wie die einzelnen Einheiten anhand der folgenden Schritte eingerichtet werden:

- „Definieren einer Benutzerrolle“ auf Seite 8
- „Definieren einer Ressourcenrichtlinie“ auf Seite 11
- „Definieren eines Authentifizierungsservers“ auf Seite 14
- „Definieren eines Authentifizierungsbereichs“ auf Seite 17
- „Definieren einer Anmelderichtlinie“ auf Seite 20

HINWEIS: Das IVE unterstützt zwei Arten von Benutzern:

- **Administratoren** – Ein *Administrator* darf die Konfigurationseinstellungen des IVE anzeigen und ändern. Das erste Administratorenkonto wird über die serielle Konsole angelegt.
- **Benutzer** – Ein *Benutzer* verwendet das IVE, um auf Firmenressourcen zuzugreifen, die vom Administrator konfiguriert wurden. Das erste Benutzerkonto (testbenutzer1) legen Sie in „Überprüfen der Verfügbarkeit für die Benutzer“ auf Seite 5 an.

Im folgenden Testszenario werden die Zugriffsverwaltungselemente des IVE in erste Linie für die Konfiguration von Zugriffsparametern für einen Benutzer verwendet. Informationen zu Systemstandardeinstellungen für Administratoren finden Sie unter „Standardeinstellungen für Administratoren“ auf Seite 26.

Definieren einer Benutzerrolle

Eine *Benutzerrolle* ist eine Einheit, die Parameter für Benutzersitzungen, individuelle Einstellungen und aktivierte Zugriffsfunktionen[1] für Benutzer definiert. Die Appliance IVE ordnet einen authentifizierten Benutzer mindestens einer Rolle zu. Die für diese Rolle(n) eingestellten Optionen legen fest, auf welche Arten von Ressourcen der Benutzer bei der IVE-Sitzung zugreifen darf.

1. Zu den Zugriffsfunktionen zählen Webbrowsing, Dateinavigation, Telnet/SSH, Network Connect und Secure Email Client.

Das IVE ist mit einem Benutzerbereich namens „Users“ vorkonfiguriert. Diese vordefinierte Rolle aktiviert die Zugriffsfunktionen für Webbrowsing und Dateinavigation, das jeder Benutzer, der der Rolle „Users“ zugeordnet ist, auf das Internet, Firmenwebserver und alle verfügbaren Windows- und UNIX/NFS-Dateiserver zugreifen darf. Diese Rolle wird auf der Seite **Users > Roles** angezeigt.

HINWEIS: Nachdem Sie eine Zugriffsfunktion für eine Rolle aktiviert haben (auf der Seite **Users > Roles >** *Rollenname*), konfigurieren Sie die entsprechenden Optionen nach Bedarf. Hierzu verwenden Sie die Konfigurationsregisterkarte der jeweiligen Zugriffsfunktion.

So definieren Sie eine Benutzerrolle:

1. Wählen Sie in der Administrator-Webkonsole **Users > Roles** aus.
2. Klicken Sie auf der Seite **Roles** auf **New Policy**.
3. Geben Sie auf der Seite **New Role** im Feld **Name** „Testrolle“ ein, und klicken Sie dann auf **Save Changes**. Warten Sie, bis das IVE die Seite **General > Overview** für die Testrolle anzeigt.
4. Aktivieren Sie auf der Seite **Overview** unter **Access Features** das Kontrollkästchen **Web**, und klicken Sie dann auf **Save Changes**.
5. Wählen Sie **Web > Options** aus.
6. Aktivieren Sie unter **Browsing** das Kontrollkästchen **User can type URLs in the IVE** browser bar, und klicken Sie dann auf **Save Changes**.

Nach Abschluss dieser Schritte haben Sie die Benutzerrolle definiert. Wenn Sie Ressourcenrichtlinien anlegen, können Sie sie dieser Rolle zuordnen. Sie können Benutzer dieser Rolle auch anhand von Rollenzuordnungsregeln, die für einen Authentifizierungsbereich definiert wurden, festlegen.

HINWEIS: Sie können eine Benutzerrolle mit aktivierten Funktionen für Webbrowsing und Dateinavigation ganz einfach anlegen, indem Sie die Rolle „Benutzer“ doppelt anlegen und dann nach Bedarf weitere Zugriffsfunktionen aktivieren.

Abbildung 4: Seite „Users > Roles > New Role“

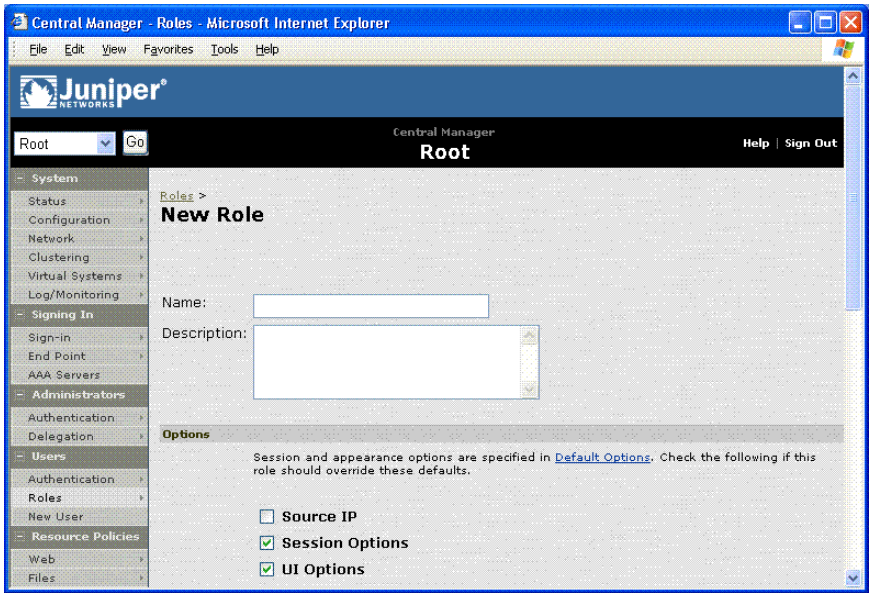
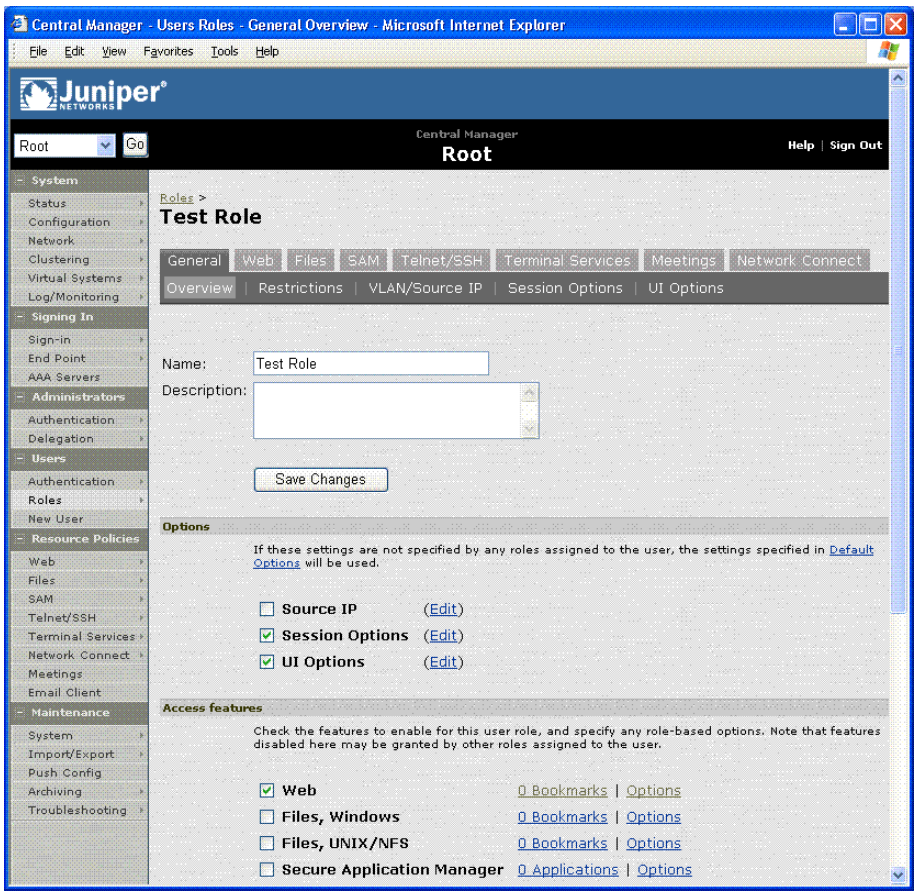


Abbildung 5: Users > Roles > Test Role > General > Overview



Definieren einer Ressourcenrichtlinie

Eine *Ressourcenrichtlinie* ist eine Systemregel, die Folgendes angibt:

- Ressourcen, für die die Richtlinie gilt (z. B. URLs, Server und Dateien)
- Benutzer, für die die Richtlinie gilt (durch Rollen oder andere Sitzungsvariablen festgelegt)
- Ob das IVE Zugriff auf eine Ressource gewährt oder eine Aktion ausführt.

Das IVE ist mit zwei Arten von Ressourcenrichtlinien vorkonfiguriert.

- **Webzugriff** – Die vordefinierte Ressourcenrichtlinie für Webzugriff erlaubt allen Benutzern, über das IVE auf das Internet and sämtliche Firmenwebserver zuzugreifen. Diese Ressourcenrichtlinie gilt standardmäßig für die Rolle „Users“.
- **Windows-Zugriff** – Die vordefinierte Ressourcenrichtlinie für Windows-Zugrifferlaubt allen Benutzern, die der Rolle „Users“ zugeordnet sind, auf sämtliche Windows-Dateiserver der Firma zuzugreifen. Diese Ressourcenrichtlinie gilt standardmäßig für die Rolle „Users“.

Sie können die Standardressourcenrichtlinien für Web- und Dateizugriff auf den Seiten **Resource Policies > Web > Access** und **Resource Policies > Files > Windows > Access** anzeigen.

HINWEIS: Wenn Sie nicht möchten, dass Benutzer auf den gesamten Web- und Dateiinhalt zugreifen können, löschen Sie die Standardressourcenrichtlinien für Web- und Dateizugriff.

So definieren Sie eine -Ressourcenrichtlinie:

1. Wählen Sie in der Administrator-Webkonsole **Resource Policies > Web > Access Control** aus.
2. Klicken Sie auf der Seite **Web Access Policies** auf **New Policy**.
3. Gehen Sie auf der Seite **New Policy** folgendermaßen vor:
   a. Geben Sie im Feld **Name** Folgendes ein: Test-Webzugriff
   b. Geben Sie im Feld **Resources** Folgendes ein: http://www.google.com
   c. Wählen Sie unter **Roles** die Option **Policy applies to SELECTED roles** und dann im Feld **Available Roles** „Testrolle“ aus. Klicken Sie anschließend auf **Add**, um sie in das Feld **Selected Roles** zu verschieben.
   d. Wählen Sie unter **Action** die Option **Deny access** aus.
   e. Klicken Sie auf **Änderungen speichern**. Das IVE fügt „Test-Webzugriff“ auf der Seite **Web Access Policies** hinzu.

4. Klicken Sie auf der Seite **Web Access Policies** in der Liste **Policies** auf das Kontrollkästchen neben „Test-Webzugriff“. Das IVE markiert die Tabellenzeile in gelb.

5. Klicken Sie oben auf der Seite auf den Pfeil nach oben , um die Zeile „Test-Webzugriff“ über der vorgegebenen Zeile „Initial Open Policy“, und klicken Sie dann auf **Save Changes**.

HINWEIS: Das IVE verarbeitet Ressourcenrichtlinien der Reihe nach und beginnt dabei mit der ersten Richtlinie in der Liste. Damit das IVE die richtigen Ressourceneinschränkungen auf Benutzer anwendet, müssen die Richtlinien in einer Ressourcenrichtlinienliste von der restriktivsten zur offensten geordnet werden. Die restriktivste Richtlinie muss dabei als erste in der Liste angegeben werden.

Nach Abschluss dieser Schritte haben Sie eine Webzugriffsressource konfiguriert. Hinweis: Auch wenn die nächste Richtlinie in der Liste der Webzugriffsrichtlinien Benutzern den Zugriff auf sämtliche Webressourcen erlaubt, ist Benutzern, die der Rolle „Users“ zugeordnet sind, der Zugriff auf den URL „http://www.google.com“ verboten. Das liegt daran, dass sie die Bedingungen der ersten Richtlinie (Test-Webzugriff) erfüllen, dir Vorrang vor der nächsten hat.

Abbildung 6: Resource Policies > Web > Access > New Policy

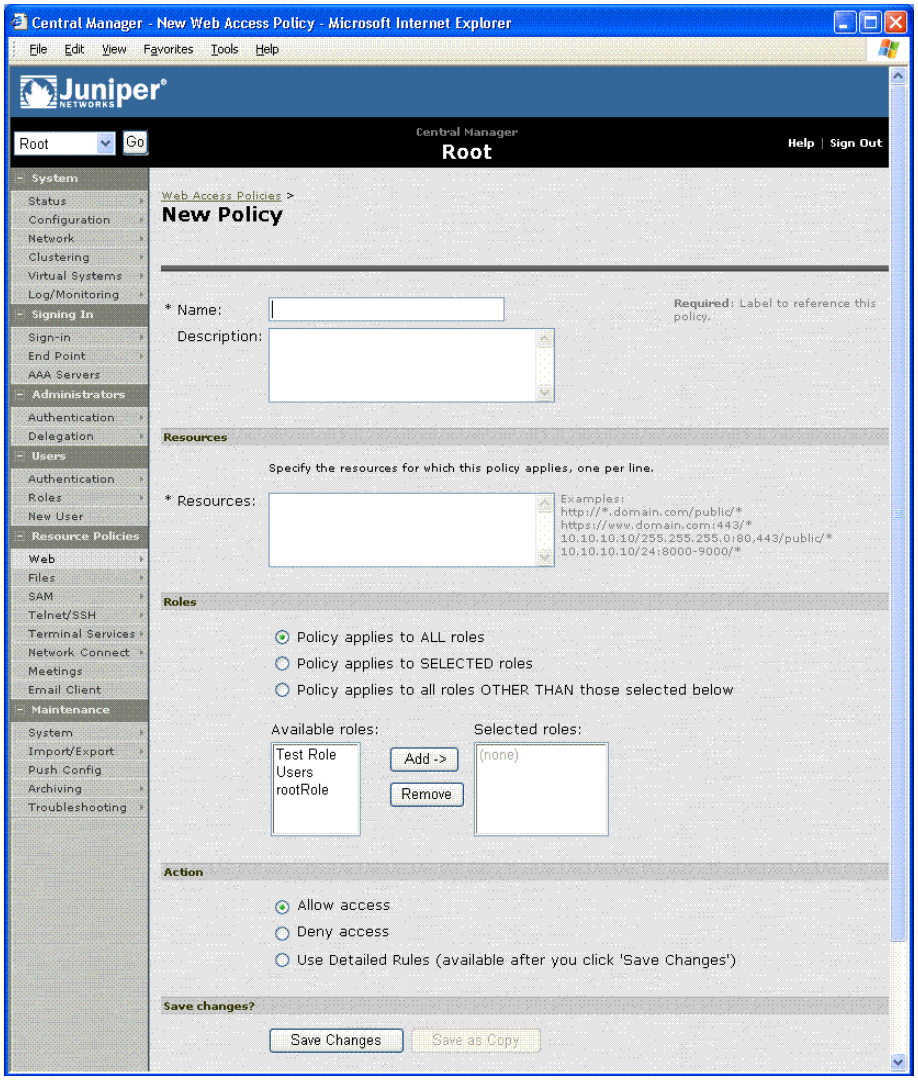
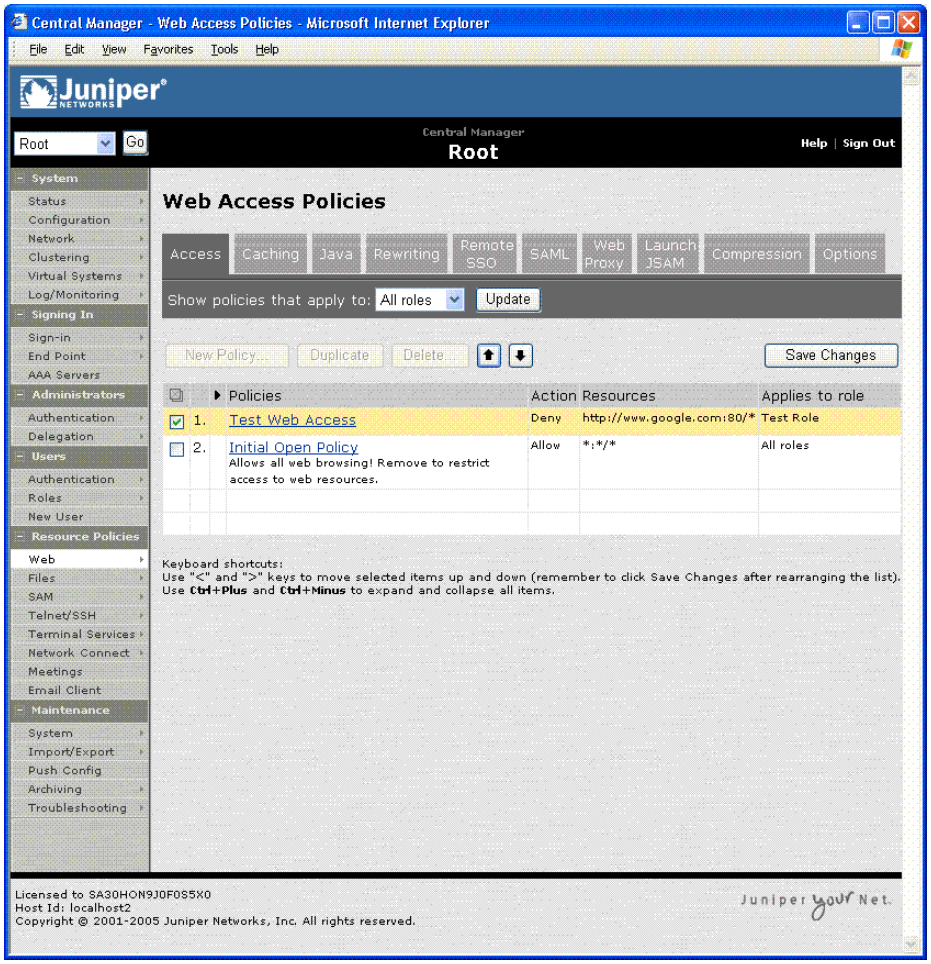


Abbildung 7: Resource Policies > Web > Access – Reihenfolge der Richtlinien ändern



Definieren eines Authentifizierungsservers

Ein *Authentifizierungsserver* ist eine Datenbank, in der Anmeldeinformationen für Benutzer (Benutzername und Kennwort) und normalerweise Gruppen- und Attributinformationen gespeichert werden. Wenn sich ein Benutzer an der IVE anmeldet, gibt er einen Authentifizierungsbereich an, der einem Authentifizierungsserver zugeordnet ist. Das IVE leitet die Anmeldeinformationen des Benutzers an diesen Authentifizierungsserver weiter, um die Identität des Benutzers zu überprüfen.

Das IVE unterstützt die gängigen Authentifizierungsserver, z. B. Windows NT-Domäne, Active Directory, RADIUS, LDAP, NIS, RSA ACE/Server und Netegrity SiteMinder. Sie können eine oder mehrere lokale Datenbanken für Benutzer anlegen, die vom IVE authentifiziert werden. Das IVE ist mit einem lokalen Authentifizierungsserver für Benutzer namens „System Local“ vorkonfiguriert. Dabei handelt es sich um eine IVE-Datenbank, mit der Sie schnell Benutzerkonten für die Benutzerauthentifizierung anlegen können. Diese Funktion gibt Ihnen Flexibilität beim Testen und beim Einrichten der Zugriffs für Dritte, da keine Benutzerkonten auf einem externen Authentifizierungsserver angelegt werden müssen.

Sie können den lokalen Authentifizierungsserver auf der Seite **Signing In > AAA Servers** anzeigen.

HINWEIS: Das IVE unterstützt auch Autorisierungsserver. Ein *Autorisierungsserver* (oder Verzeichnisserver) ist eine Datenbank, in der Benutzerattribut- und -gruppeninformationen gespeichert werden. Sie können einen Authentifizierungsbereich so konfigurieren, dass ein Verzeichnisserver Benutzerattribut- oder -gruppeninformationen abruft, die in Rollenzuordnungsregeln und Ressourcenrichtlinien verwendet werden.

So definieren Sie einen Authentifizierungsserver:

1. Wählen Sie in der Administrator-Webkonsole **Signing In > AAA Servers** aus.

2. Wählen Sie auf der Seite **Authentication Servers** in der Liste **New** die Option **IVE** Authentication aus, und klicken Sie dann auf **New Server**.

3. Geben Sie auf der Seite **New IVE Authentication** im Feld **Name** „Testserver“ ein, und klicken Sie dann auf **Save Changes**. Warten Sie, bis das IVE Ihnen meldet, dass die Änderungen gespeichert wurden. Anschließend werden weitere Konfigurationsregisterkarten angezeigt.

4. Klicken Sie auf die Registerkarte **Users** und dann auf **New**.

5. Geben Sie auf der Seite **New Local User** im Feld **Username** „testbenutzer2“ ein, geben Sie ein Kennwort ein, und klicken Sie dann auf **Save Changes**, um das Benutzerkonto im Authentifizierungsserver „Testserver“ anzulegen.

Nach dem Abschluss dieser Schritte haben Sie einen Authentifizierungsserver mit einem Benutzerkonto angelegt. Dieser Benutzer kann sich an einem Authentifizierungsbereich anmelden, der den Authentifizierungsserver „Testserver“ verwendet.

Abbildung 8: Signing In > AAA Servers > New Server

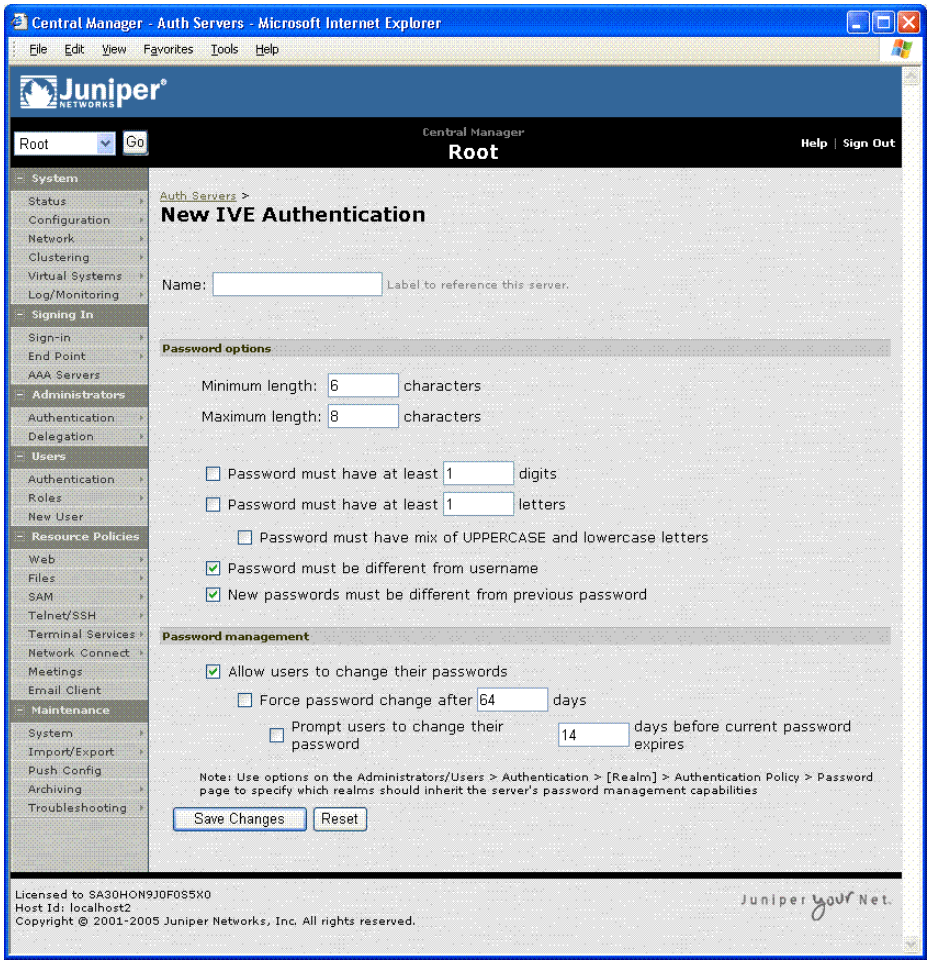


Abbildung 9: Signing In > AAA Servers > Test Server > Users > New

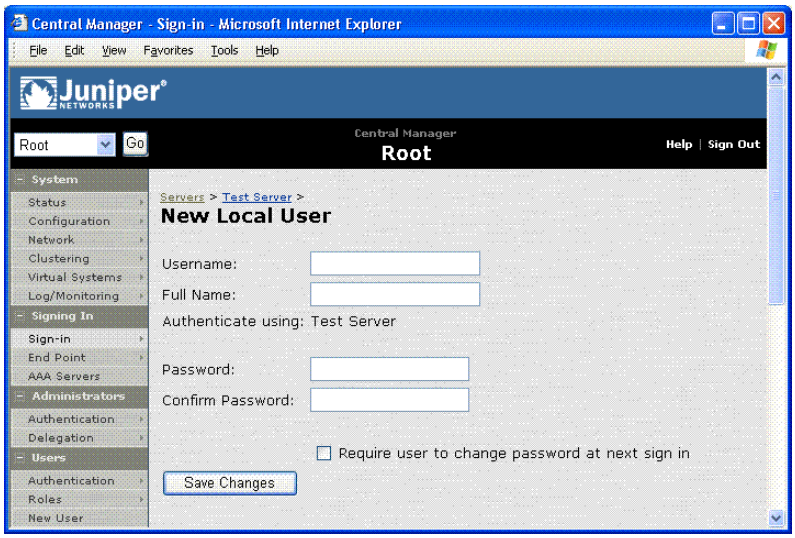
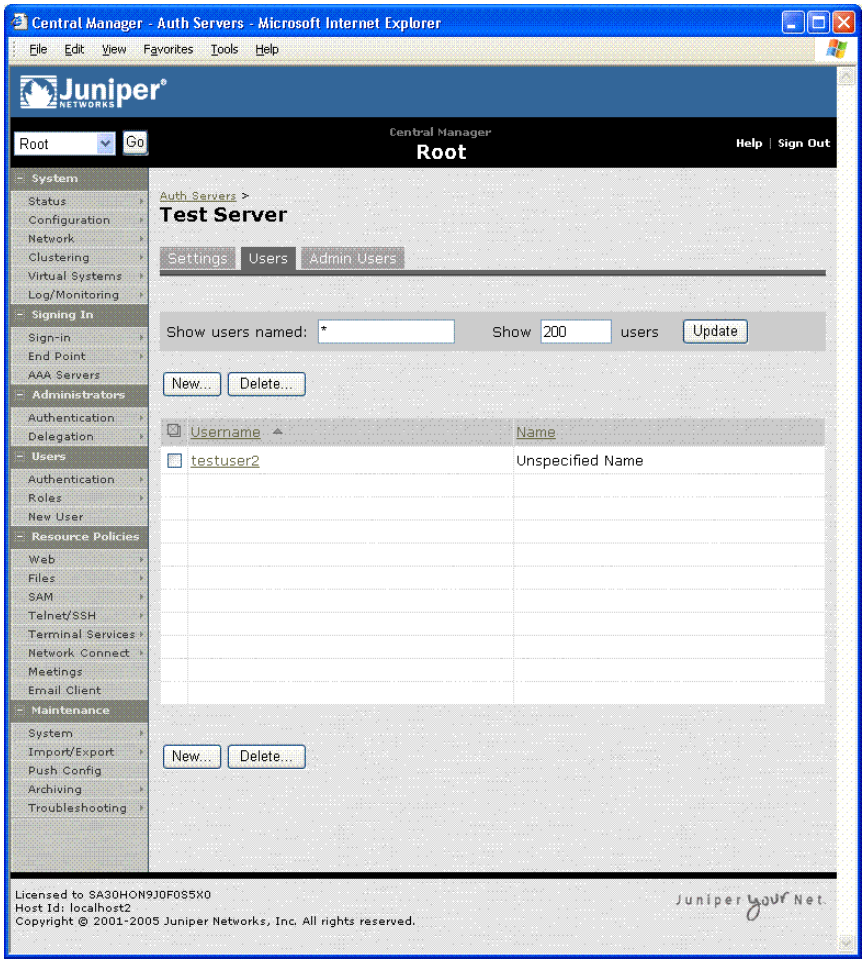


Abbildung 10: Signing In > AAA Servers > Test Server > Users



Definieren eines Authentifizierungsbereichs

Als *Authentifizierungsbereich* wird eine Gruppierung von Authentifizierungsressourcen bezeichnet, einschließlich:

- Einen Authentifizierungsserver, der die Identität des Benutzers überprüft. Das IVE leitet die Anmeldeinformationen, die von einer Anmeldeseite abgesendet wurden, an einen Authentifizierungsserver weiter.
- Eine Authentifizierungsrichtlinie, die die Sicherheitsanforderungen des Bereichs angibt, die erfüllt sein müssen, damit das IVE die Anmeldeinformationen eines Benutzers zur Überprüfung an einen Authentifizierungsserver weiterleitet.
- Einen Verzeichnisserver, d. h. einen LDAP-Server, der dem IVE Benutzer- und Gruppenattributinformationen bereitstellt, die für Rollenzuordnungsregen und Ressourcenrichtlinien verwendet werden.

- Rollenzuordnungsregeln, die die Bedingungen angeben, die ein Benutzer erfüllen muss, damit ihn das IVE einer oder mehreren Rollen zuweist. Diese Bedingungen beruhen auf Informationen, die der Verzeichnisserver des Bereichs zurückgibt, dem Benutzernamen des Benutzers oder Zertifikatattributen.

Das IVE ist mit einem Benutzerbereich namens „Users“ vorkonfiguriert. Dieser vordefinierte Bereich verwendet den Authentifizierungsserver „System Local“, eine Authentifizierungsrichtlinie, bei der eine Mindestkennwortlänge von vier Zeichen und kein Verzeichnisserver gegeben sein müssen. Sie enthält eine Rollenzuordnungsregel, die alle Benutzer, die sich am Bereich „Users“ anmelden, der Rolle „Users“ zuordnet. Das Konto „testbenutzer1“, das Sie in „Überprüfen der Verfügbarkeit für die Benutzer“ auf Seite 5 anlegen, gehört zum Bereich „Users“, da dieses Konto auf dem Authentifizierungsserver „System Local“ angelegt wird. Das Konto „testbenutzer2“, das Sie in „Definieren eines Authentifizierungsservers“ auf Seite 14 anlegen, gehört **nicht** zum Bereich „Users“, da dieses Konto auf dem Authentifizierungsserver „Testserver“ angelegt wird, der vom Bereich „Users“ nicht verwendet wird.

Sie können den lokalen Standard-Authentifizierungsbereich für Benutzer auf der Seite **Users > Authentication** anzeigen.

So definieren Sie einen Authentifizierungsbereich:

1. Wählen Sie in der Administrator-Webkonsole **Users > Authentication** aus.
2. Klicken Sie auf der Seite **User Authentication Realms** auf **New**.
3. Gehen Sie auf der Seite **New Authentication Realm** folgendermaßen vor:
   a. Geben Sie im Feld **Name** Folgendes ein: Testbereich
   b. Wählen Sie unter **Servers** in der Liste **Authentication** den Eintrag „Testserver“ aus.
   c. Klicken Sie auf **Änderungen speichern**. Warten Sie, bis das IVE Ihnen meldet, dass die Änderungen gespeichert wurden. Anschließend werden die Konfigurationsregisterkarten für den Bereich angezeigt.
4. Klicken Sie auf der Registerkarte **Role Mapping** auf **New Rule**.
5. Gehen Sie auf der Seite **Role Mapping Rule** folgendermaßen vor:
   a. Geben Sie unter **Rule: If username...** „testbenutzer2“ in das Wertfeld ein.
   b. Wählen Sie unter **...then assign these roles** im Feld **Available Roles** „Testrolle“ aus, und klicken Sie dann auf **Add**, um sie in das Feld **Selected Roles** zu verschieben.
   c. Klicken Sie auf **Änderungen speichern**.

Nach Abschluss dieser Schritte haben Sie einen Authentifizierungsbereich definiert. Dieser Bereich verwendet „Testserver“ für die Benutzerauthentifizierung und eine Rollenzuordnungsregel, um „testbenutzer2“ zu „Testrolle“ zuzuordnen. Da für „Testrolle“ die Ressourcenrichtlinie „Test-Webzugriff“ gilt, können die Benutzer, die dieser Rolle zugeordnet sind, nicht auf „http://www.google.com“ zugreifen.

Abbildung 11: Users > Authentication > New Realm

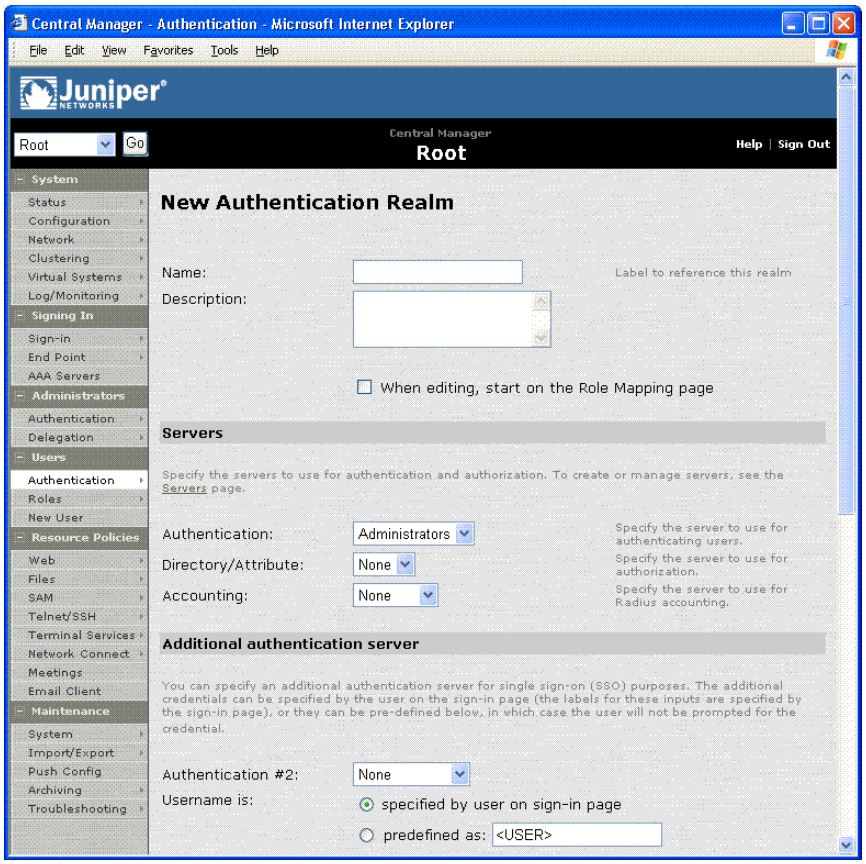
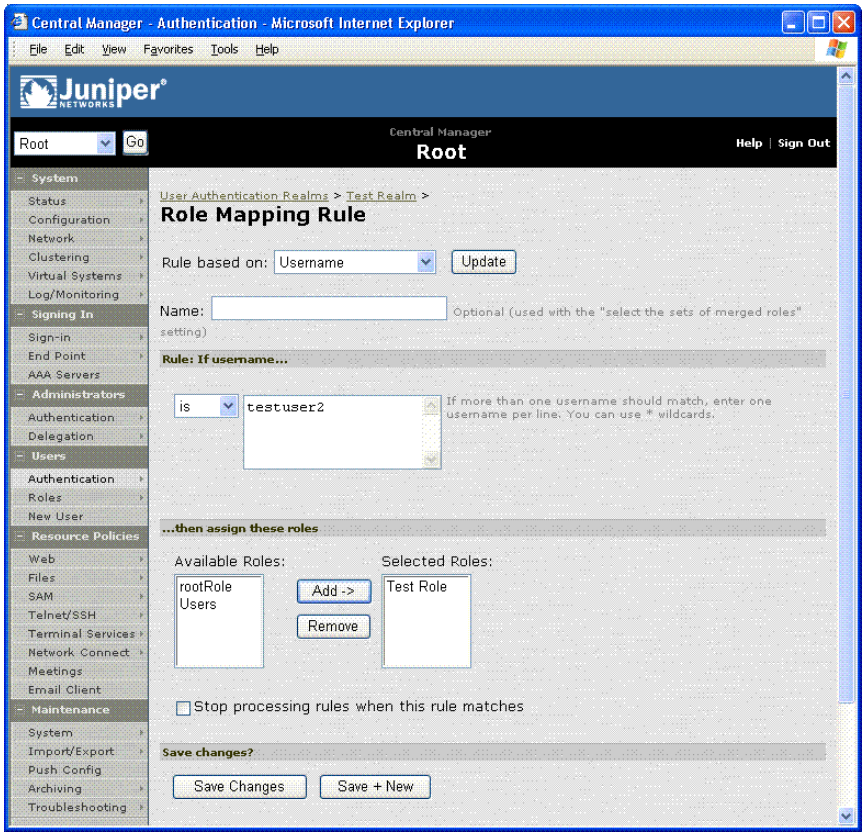


Abbildung 12: Users > Authentication > Testserver > New Rule



Definieren einer Anmelderichtlinie

Eine *Anmelderichtlinie* ist eine Systemregel, die Folgendes angibt:

- einen URL, unter dem sich ein Benutzer am IVE anmelden kann
- eine Anmeldeseite, die für den Benutzer angezeigt wird
- ob der Benutzer einen Authentifizierungsbereich eingeben oder auswählen muss, an den das IVE die Anmeldeinformationen sendet
- die Authentifizierungsbereiche, für die die Anmelderichtlinie gilt

Alle Access Series und Access Series FIPS IVEs sind mit einer Anmelderichtlinie vorkonfiguriert, die für Benutzer gilt: ***/** . Diese Standard-Anmelderichtlinie für Benutzer (*/) legt Folgendes fest: Wenn ein Benutzer den URL für das IVE eingibt, zeigt das IVE die Standard-Anmeldeseite für Benutzer an und fordert den Benutzer zur Auswahl eines Authentifizierungsbereichs auf (sofern mehrere Bereiche vorhanden sind). Die Anmelderichtlinie */ gilt für den Authentifizierungsbereich „Users“ und gilt daher **nicht** für den Authentifizierungsbereich, den Sie im Schritt „Definieren eines Authentifizierungsbereichs“ auf Seite 17 anlegen.

Sie können die Standard-Anmelderichtlinie für Benutzer auf der Seite **Signing In** > **Sign-in** > Sign-in Policies anzeigen.

Die Standard-Anmelderichtlinie gilt für alle Benutzer. Sie können den URL der IVE-Anmeldeseite für Benutzer ändern, indem Sie zum Pfad beispielsweise „*/mitarbeiter“ hinzufügen, Sie können jedoch keine weiteren Anmelderichtlinien hinzufügen. Hierfür müssen Sie die Lizenz „Advanced“ für das IVE erwerben.

So definieren Sie eine Anmelderichtlinie:

1. Wählen Sie in der Administrator-Webkonsole **Signing In > Sign-in > Sign-in Policies** aus.

2. Klicken Sie auf der Seite **Sign-in Policies** auf ***/**.

3. Gehen Sie auf der Seite ***/** folgendermaßen vor:

   a. Geben Sie im Feld **Sign-in URL** nach „*/“ den Eintrag „Test“ ein:

   b. Aktivieren Sie unter **Authentication realm** die Option **User picks from a list of authentication realms**, und wählen Sie dann im Feld **Available Roles** „Testbereich“ aus. Klicken Sie anschließend auf **Add**, um den Bereich in das Feld **Selected Realms** zu verschieben. (Wiederholen Sie diesen Vorgang für die Rolle „Users“, sofern sich diese nicht bereits im Feld **Selected Realms** befindet.)

   c. Klicken Sie auf **Änderungen speichern**.

Nach Abschluss dieser Schritte haben Sie die Bearbeitung der Standard-Anmelderichtlinie für Benutzer definiert.

Optional:

1. Wählen Sie **Signing In > Sign-in > Sign-in Pages** aus, und klicken Sie dann auf **New Page**.

2. Geben Sie auf der Seite **New Sign-In Page** im Feld **Name** „Test-Anmeldeseite“ ein, geben Sie im Feld **Background color** „#FF0000“ (rot) ein, und klicken Sie dann auf **Save Changes**.

3. Wählen Sie **Signing In > Sign-in > Sign-in Policies** aus, und klicken Sie dann auf **New URL**.

4. Geben Sie auf der Seite **New Sign-in Policy** „*/test/“ in das Feld **Name** ein, aktivieren Sie im Feld **Sign-in Page** die Option **Default Sign-in Page**, und klicken Sie auf **Save Changes**.

5. Wählen Sie **Signing In > Sign-in > Sign-in Policies** aus, und klicken Sie dann unter **User URLs** auf ***/test/**.

6. Wählen Sie auf der Seite ***/test/** aus der Liste **Sign-in page** „Test-Anmeldeseite“ aus, und klicken Sie dann auf **Save Changes**.

Nach Abschluss dieser optionalen Schritte haben Sie eine neue Anmeldeseite definiert, die der Anmelderichtlinie „*/test/“ zugeordnet ist.

Abbildung 13: Signing In > Sign-in > Sign-in Policies > */

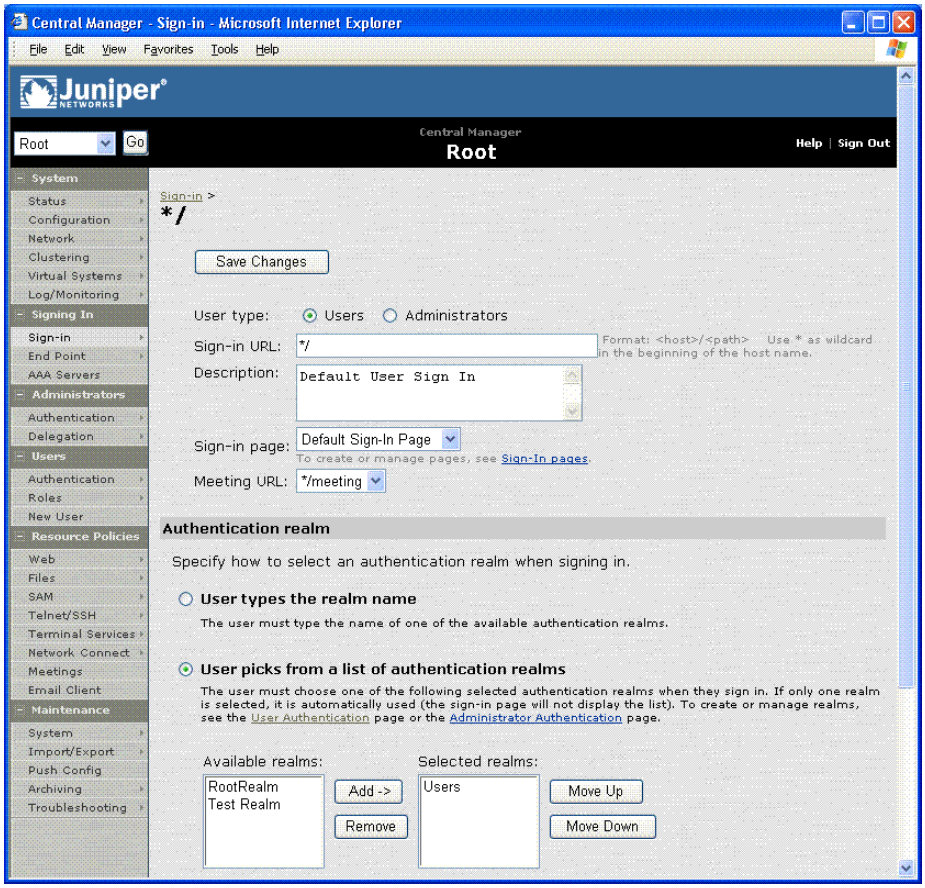
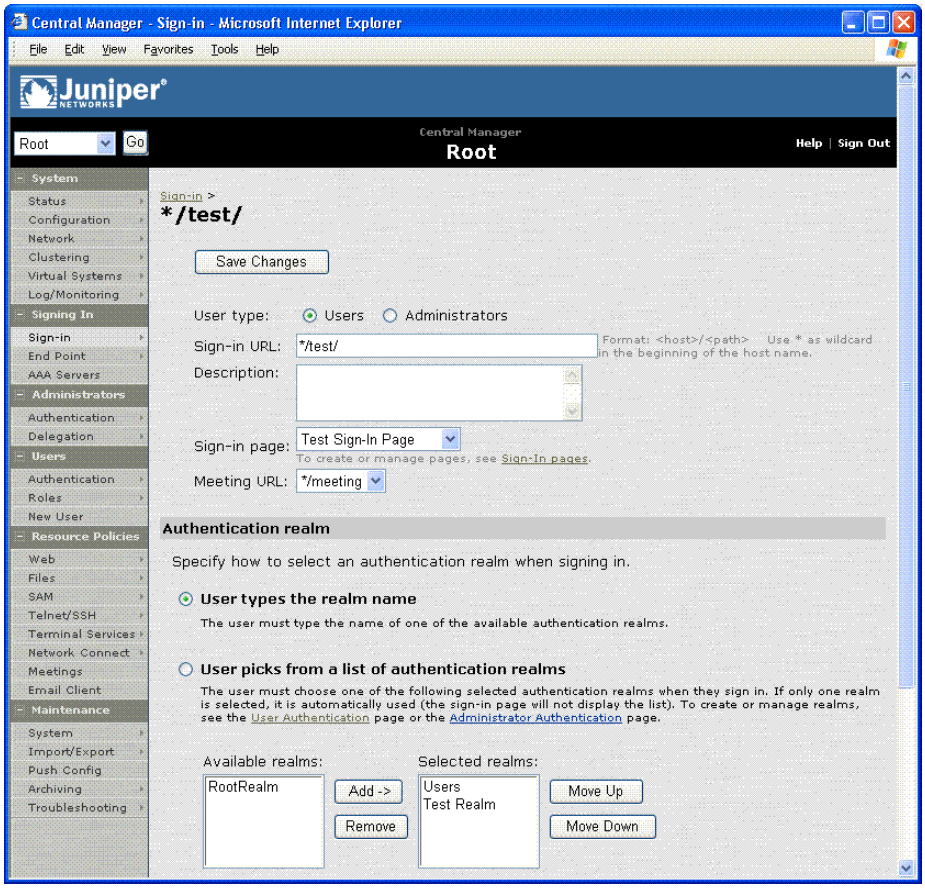


Abbildung 14: Signing In > Sign-in > Sign-in Policies > */test/ — Verwenden der Seite „New Sign-in“



Verwenden des Testszenarios

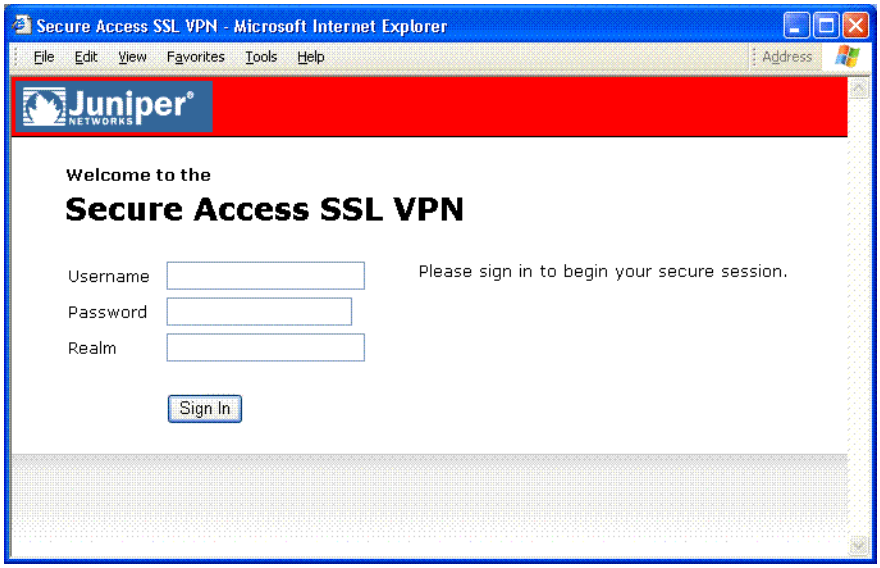
Dieses Testszenario gibt Ihnen folgende Möglichkeiten:

- Zugriff auf die Benutzer-Webkonsole über die geänderte Standard-Anmelderichtlinie
- Anmeldung am Testbereich als der Benutzer, der in „Testserver“ erstellt wurde
- Testen der Webbrowsing-Funktionen, die von der ordnungsgemäßen Konfiguration von der Testrolle und dem Test-Webzugriff abhängen

So verwenden Sie das Testszenario:

1. Öffnen Sie die Benutzer-Anmeldeseite, indem Sie in einem Browser den Geräte-URL, gefolgt von „/test“ eingeben. Der URL weist folgendes Format auf: `https://a.b.c.d/test`, wobei `a.b.c.d` die IP-Adresse des Geräts ist, die Sie während der Erstkonfiguration in der seriellen Konsole eingegeben haben. Wenn Sie in einer Sicherheitswarnung gefragt werden, ob Sie ohne signiertes Zertifikat fortfahren möchten, klicken Sie auf **Yes**. Wenn die Benutzer-Anmeldeseite angezeigt wird, haben Sie das IVE ordnungsgemäß mit dem Netzwerk verbunden.

Abbildung 15: Benutzer-Anmeldeseite

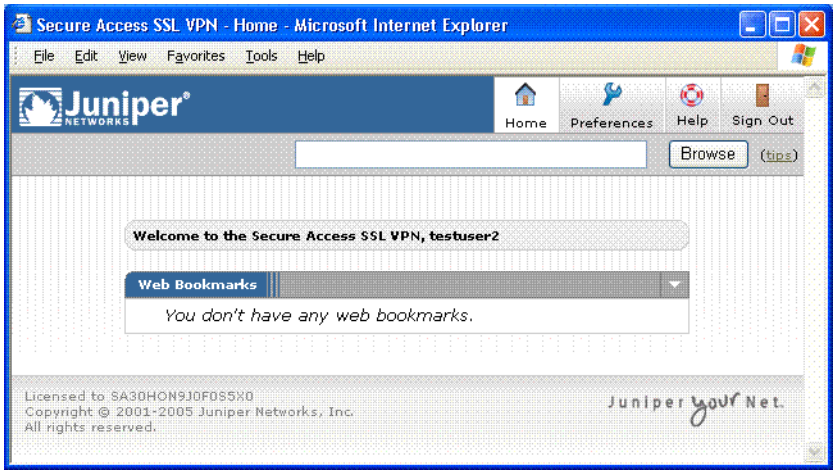


HINWEIS: Wenn Sie in „Definieren einer Anmelderichtlinie“ auf Seite 20 die optimale Konfigurationsschritte durchgeführt haben, wird der Header in rot angezeigt.

2. Geben Sie auf der Anmeldeseite die Anmeldeinformationen (Benutzername und Kennwort) ein, die Sie für das Benutzerkonto in „Testserver“ angelegt haben, wählen Sie im Feld **Realm** „Testbereich“ aus, und klicken Sie dann auf **Sign In**, um die IVE-Benutzerstartseite zu öffnen.

   Das IVE leitet die Anmeldeinformationen an „Testbereich“ weiter, der für die Verwendung von „Testserver“ konfiguriert ist. Nach der erfolgreichen Überprüfung durch diesen Authentifizierungsserver verarbeitet das IVE die Rollenzuordnungsregel, die für „Testbereich“ definiert ist. Dieser ordnet „testbenutzer2“ zur „Testrolle“ zu. Die Testrolle erlaubt Benutzern das Webbrowsing.

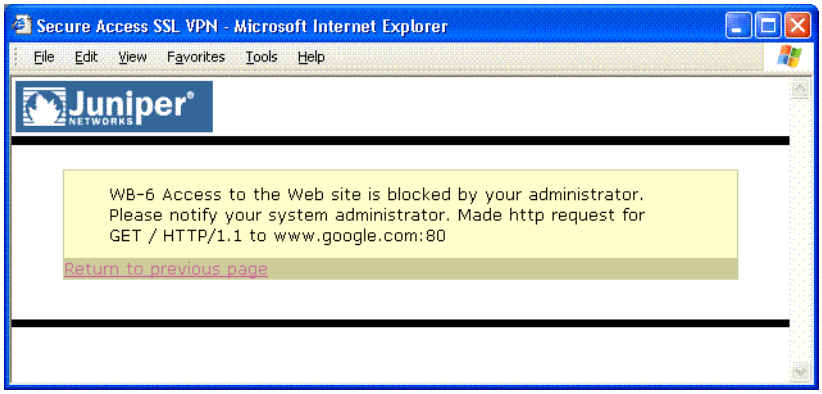
Abbildung 16: Benutzerstartseite



3. Geben Sie im Feld **Address** des Browsers den URL zur Firmenwebsite ein, und klicken Sie auf **Browse**. Das IVE öffnet die Webseite in demselben Browserfenster. Kehren Sie daher zur IVE-Startseite zurück, und klicken Sie auf der Navigationssymbolleiste, die auf der Zielwebseite angezeigt wird, auf das Symbol in der Mitte.

4. Geben Sie auf der IVE-Startseite „www.google.com“ ein, und klicken Sie auf **Browse**. Das IVE zeigt eine Fehlermeldung an, da die Ressourcenrichtlinie „Test-Webzugriff“ Benutzern, die der „Testrolle“ zugeordnet sind, den Zugriff auf diese Site verweigert.

Abbildung 17: Beispiel für eine Fehlermeldung bei Zugriffsverweigerung


Secure Access SSL VPN - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Juniper NETWORKS
WB-6 Access to the Web site is blocked by your administrator.
Please notify your system administrator. Made http request for
GET / HTTP/1.1 to www.google.com:80
Return to previous page

5. Kehren Sie auf die IVE-Startseite zurück, klicken Sie auf **Sign Out**, und kehren Sie dann auf die Benutzer-Anmeldeseite zurück.

6. Geben Sie die Anmeldeinformationen für „testbenutzer1“ ein, wählen Sie den Bereich **Users** aus, und klicken Sie dann auf **Sign In**.

7. Geben Sie auf der IVE-Startseite „www.google.com“ ein, und klicken Sie auf **Browse**. Das IVE öffnet die Webseite in demselben Browserfenster.

Das Testszenario veranschaulicht die grundlegenden IVE-Mechanismen der Zugriffsverwaltung. Sie können ausgefeilte Rollenzuordnungsregeln und Ressourcenrichtlinien anlegen, mit denen der Benutzerzugriff anhand von Elementen wie der Authentifizierungsrichtlinie eines Bereichs, der Gruppenmitgliedschaft eines Benutzers und anderen Variablen gesteuert werden kann. Wenn Sie sich intensiver mit der IVE-Zugriffsverwaltung befassen möchten, sollten Sie sich etwas Zeit nehmen und sich mit den Themen der Onlinehilfe vertraut machen.

HINWEIS:

- Wenn Sie das IVE für Ihr Unternehmen konfigurieren, empfehlen wir Ihnen, bei der Konfiguration des Benutzerzugriff die in diesem Abschnitt dargestellte Reihenfolge einzuhalten.
- Ausführliche Informationen zur Konfiguration können Sie der Onlinehilfe oder dem Administratorhandbuch (im PDF-Format) entnehmen, auf den Sie über die Onlinehilfe oder über die Support-Site zugreifen können.
- Bevor Sie den Zugriff auf Ihr IVE von externen Standorten freigeben, empfehlen wir Ihnen, ein signiertes digitales Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zu importieren.

Standardeinstellungen für Administratoren

Das IVE bietet Ihnen, genau wie den Benutzern, Standardeinstellungen, mit denen Sie schnell Administratorkonten konfigurieren können. In dieser Liste werden die Systemstandardeinstellungen für Administratoren aufgeführt:

- **Administratorrollen**
  - **.Administrators** – Diese vorkonfigurierte Rolle erlaubt Administratoren die Verwaltung sämtlicher Aspekte des IVE. Der Administrator-Benutzer, den Sie über die serielle Konsole anlegen, wird dieser Rolle zugeordnet.
  - **.Read-Only Administrators** – Diese vorkonfigurierte Rolle erlaubt es den zugeordneten Benutzern, sämtliche Einstellungen des IVE anzuzeigen, jedoch nicht zu konfigurieren. Wenn Sie den Zugriff von Administratoren einschränken möchten, müssen Sie sie dieser Rolle zuordnen.

HINWEIS: Zum Anlegen weiterer Administratorrollen benötigen Sie die Lizenz „Advanced“.

- **Lokaler Authentifizierungsserver „Administrators“** – Der Administrator-Authentifizierungsserver ist eine IVE-Datenbank, in der die Administratorkonten gespeichert werden. Das erste Administratorenkonto in diesem Server wird über die serielle Konsole angelegt. (Das IVEfür alle Administratorenkonten, die über die serielle Konsole angelegt wurden, zu diesem Server hinzu.) Dieser lokale Server kann nicht gelöscht werden.

- **Authentifizierungsbereich „Admin Users“** – Der Authentifizierungsbereich „Admin Users“ verwendet den Standard-Authentifizierungsserver „Administrators“, eine Authentifizierungsrichtlinie mit einer Mindestkennwortlänge von vier Zeichen und keinen Verzeichnisserver. Er enthält eine Rollenzuordnungsregel, die alle Benutzer, die sich am Bereich „Admin Users“ anmelden, der Rolle „Administrators“ zuordnet. Das Administratorkonto, das Sie über die serielle Konsole anlegen, gehört zum Bereich „Admin Users“.

- **Anmelderichtlinie „*/“** – Die Standard-Anmelderichtlinie für Administratoren (*/admin) legt Folgendes fest: Wenn ein Benutzer den URL zum IVE, gefolgt von „`/admin`“ eingibt, zeigt das IVE die Standard-Anmeldeseite für Administratoren an. Außerdem muss der Administrator einen Authentifizierungsbereich auswählen (sofern mehrere Bereiche vorhanden sind). Die Anmelderichtlinie „*/“ gilt für den Authentifizierungsbereich „Admin Users“ und gilt daher für das Administratorkonto, das Sie über die serielle Konsole anlegen.

Teil 2

IVE Produkte und Funktionen

Dieser Abschnitt bietet einen Überblick über IVE-Produkte und -Funktionen. Die IVE-Plattform, auf der die Secure Access 700-Appliance basiert, Standardfunktionen aller auf der IVE-Plattform basierenden Produkte und individuelle IVE-Funktionen werden beschrieben.

Inhalt

- „Authentifizierung und Autorisierung“ auf Seite 63
- „Remotezugriff“ auf Seite 93
- „Systemverwaltung und Systemdienste“ auf Seite 121

Kapitel 2

Die IVE-Reihe

In diesem Abschnitt werden die NetScreen IVE-Plattform (Instant Virtual Extranet), die Access Series-Produktlinien, die auf dieser Plattform aufbauen, und das Zugriffsverwaltungssystem beschrieben, das von den auf der IVE-Plattform aufbauenden Produkten verwendet wird.

Inhalt

- „Einführung in die NetScreen Instant Virtual Extranet-Plattform“ auf Seite 33
- „Access Series – Übersicht“ auf Seite 37
- „Zugriffsverwaltung – Übersicht“ auf Seite 38
- „Authentifizierungsbereiche – Übersicht“ auf Seite 51
- „Anmelderichtlinien – Übersicht“ auf Seite 55
- „Benutzerrollen – Übersicht“ auf Seite 56
- „Ressourcenrichtlinien – Übersicht“ auf Seite 59

Einführung in die NetScreen Instant Virtual Extranet-Plattform

Die NetScreen Instant Virtual Extranet (IVE) -Plattform liegt den Juniper Networks NetScreen SSL VPN -Appliances als Hard- und Software zugrunde. Mit diesen Produkten können Sie Mitarbeitern, Partnern und Kunden über einen beliebigen Webbrowser überall sicheren und kontrollierten Zugriff auf die Ressourcen Ihres Unternehmens gewähren!

Weitere Informationen finden Sie unter:

- „Was ist die IVE-Plattform?“ auf Seite 33
- „Wie bauen Produkte auf der Funktionsweise der IVE-Plattform auf?“ auf Seite 34
- „Aufgabenzusammenfassung: Konfigurieren von Produkten auf Basis der IVE-Plattform“ auf Seite 35

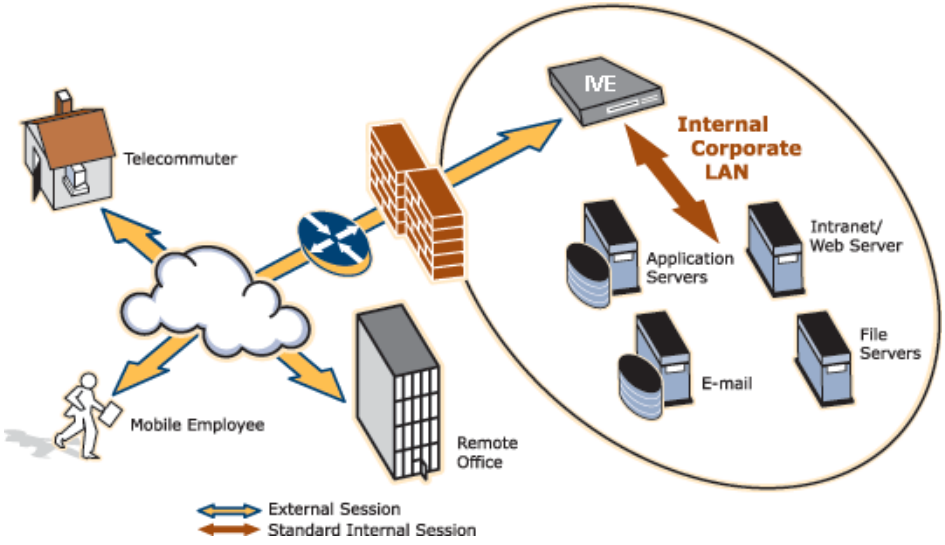
Was ist die IVE-Plattform?

Die IVE-Plattform ist eine so genannte Netzwerkappliance, die stabile Sicherheit bietet, indem sie als Zwischenglied für die Datenströme fungiert, die zwischen externen Benutzern und internen Ressourcen übertragen werden. Zu diesen gehören:

- MS Terminal-Server
- MS Exchange-Server
- Lotus Notes-Server
- Internet-E-Mail-Server
- Terminalbasierte Anwendungen
- Dokumente auf Dateiservern
- Webbasierte Unternehmensanwendungen
- Intranetseiten

Mit Produkten, die auf der IVE-Plattform aufbauen, wird es überflüssig, in einer herkömmlichen DMZ Toolkits für Extranets bereitzustellen oder den Mitarbeitern ein VPN (Virtual Private Network) für Remotezugriffe zur Verfügung zu stellen. Das IVE vermittelt Daten zwischen externen Verbindungen, über die es sichere Anforderungen erhält, und internen Ressourcen, an die es Anforderungen für authentifizierte Benutzer sendet.

Abbildung 18: Das IVE innerhalb eines LAN



Wie bauen Produkte auf der Funktionsweise der IVE-Plattform auf?

Das IVE-Plattform arbeitet als sicheres Gateway auf Anwendungsebene, das sämtliche Anforderungen zwischen dem öffentlichen Internet und internen Unternehmensressourcen vermittelt. Auf sämtliche Anforderungen, die das IVE erhält, wurde bereits durch den Browser des Endbenutzers eine 128-Bit- oder 168-Bit-SSL/HTTPS-Verschlüsselung angewendet. Unverschlüsselte Anforderungen werden verworfen. Jede Anforderung unterliegt der vom Administrator definierten Zugriffssteuerung, bei der z. B. 2-Faktor-Authentifizierung oder clientseitige digitale Zertifikate eingesetzt werden, bevor sie an die internen Ressourcen weitergeleitet wird. Da die IVE-Plattform eine stabile Sicherheitsschicht zwischen dem öffentlichen Internet und den internen Ressourcen zur Verfügung stellt, müssen Administratoren nicht fortwährend Sicherheitsrichtlinien verwalten und Sicherheitslücken für zahlreiche verschiedene Anwendungen und Webserver beheben, die in dem öffentlichen DMZ bereitgestellt werden.

Die IVE-Plattform vermittelt den Zugriff auf verschiedenste Arten von Anwendungen und Ressourcen mithilfe einfacher Webbrowsertechnologien. Die Benutzer erhalten über eine durch die Appliance gehostete Extranetsitzung einen authentifizierten Zugriff auf autorisierte Ressourcen. Benutzer können von jedem Webbrowser mit Internetanbindung über eine sichere Websitzung auf umfangreiche webbasierte Unternehmensanwendungen, Java-Anwendungen, Dateifreigaben, Terminalhosts und weitere Client/Server-Anwendungen (wie z. B. Microsoft Outlook und Lotus Notes) zugreifen.

Aufgabenzusammenfassung: Konfigurieren von Produkten auf Basis der IVE-Plattform

Die Konfiguration der IVE-Plattform erfolgt in fünf grundlegenden Schritten über die Webkonsole des Administrators:

1. **Definieren von Benutzer- und Administratorrollen**

   Speicherort auf der Webkonsole: **User > Roles** und **Administrators > Delegation**

   Rollen definieren Sitzungsparameter von Benutzern (Sitzungseinstellungen und -optionen), individuelle Einstellungen (benutzerdefinierte Einrichtung der Oberfläche und Lesezeichen) und aktivierte Zugriffsfunktionen. Eine Zugriffsfunktion ist ein Mechanismus, der den Zugriff auf Ihr Netzwerk ermöglicht, z. B. die vom Secure Access 700 verwendete Network Connect-Funktion.

   Das IVE ist bereits mit einer Benutzerrolle („Users") und zwei Administratorenrollen („.Administrators" und „.Read-Only Administrators") vorkonfiguriert.

2. **Definieren von Ressourcenrichtlinien**

   Speicherort auf der Webkonsole: **Resource Policies**

   Ressourcenrichtlinien dienen zur weitergehenden Steuerung der Ressourcen, auf die Benutzer und Administratoren zugreifen können. Sie können, z. B. eine Ressourcenrichtlinie für die Network Connect-Zugriffssteuerung definieren, die Partnern den Zugriff auf Ihre Netzwerkdateiserver verweigert. Bei der Konfiguration einer Ressourcenrichtlinie müssen Sie die Rollen angeben, für die die Ressourcenrichtlinie gelten soll.

   Auf einer Secure Access 700-Appliance ist bereits eine Ressourcenrichtlinie vorkonfiguriert, die allen Benutzern den Zugriff auf das Netzwerk gewährt.

3. **Definieren von Authentifizierungs- und Autorisierungsservern**

   Speicherort auf der Webkonsole: **Signing In > AAA Servers**

   Authentifizierungs- und Autorisierungsserver authentifizieren Anmeldeinformationen und ermitteln die Benutzerberechtigungen innerhalb des Systems. Sie können z. B. Benutzer anhand der clientseitigen Zertifikatsattribute über einen Zertifikatsserver authentifizieren und dann einen LDAP-Server verwenden, der Benutzer anhand der Werte autorisiert, die in einer Zertifikatsperrliste (Certificate Revocation List, CRL) aufgeführt sind.

   Auf dem IVE sind bereits ein lokaler Authentifizierungsserver („System Local") für die Benutzerauthentifizierung und ein lokaler Authentifizierungsserver („Administrators") für die Administratorauthentifizierung vorkonfiguriert. Sie müssen also zumindest diesen Servern Benutzer hinzufügen, damit Benutzer auf die Appliance zugreifen können.

4. **Definieren des Authentifizierungsbereichs**

   Speicherort auf der Webkonsole: **Users > Authentication** und **Administrators > Authentication**

   Authentifizierungsbereiche enthalten Richtlinien, die die Bedingungen festlegen, die Benutzer und Administratoren für die Anmeldung beim IVE erfüllen müssen. Sie können z. B. anhand einer Authentifizierungsrichtlinie angeben, dass Benutzer nur auf die Appliance zugreifen können, wenn sie sich von einer bestimmten IP-Adresse aus anmelden oder einen bestimmten Browser verwenden. Beim Konfigurieren eines Authentifizierungsbereichs müssen Sie Regeln erstellen, um Benutzer Rollen zuzuordnen und festzulegen, welche(n) Server die Appliance für die Authentifizierung und Autorisierung der Bereichsmitglieder verwenden darf.

   Auf dem IVE ist bereits ein Bereich („Users“) vorkonfiguriert, der alle über den Server „System Local“ authentifizierten Benutzer der Rolle „Users“ zuordnet. Außerdem ist auf einer Appliance bereits ein Bereich („Admin Users“) vorkonfiguriert, der alle über den Server „Administrators“ authentifizierten Benutzer der Rolle „.Administrators“ zuordnet.

5. **Definieren von Anmelderichtlinien**

   Speicherort auf der Webkonsole: **Signing In > Sign-in > Sign-In Policies**

   Anmelderichtlinien geben URLs an, die Benutzer und Administratoren für die Anmeldung beim IVE verwenden können. Bei der Konfiguration einer Anmelderichtlinie müssen Sie diese mindestens einem Bereich zuordnen. Es können sich dann nur Mitglieder des angegebenen Bereichs bzw. der angegebenen Bereiche anhand des URL, der in der Richtlinie angegeben wurde, an der Appliance anmelden.

   Auf dem IVE ist bereits eine Anmelderichtlinie vorkonfiguriert, die den Benutzern des Bereichs „Users” erlaubt, sich anhand des „*/” URL, und Mitgliedern des Bereichs „Admin Users” erlaubt, sich anhand des „*/admin” URL anzumelden.

Access Series – Übersicht

Juniper Networks NetScreen Secure Access bietet Sicherheitsfunktionen, die den sicheren Remotezugriff auf Netzwerkressourcen verbessern. Eine Secure Access 700-Appliance kann innerhalb weniger Stunden konfiguriert werden, um Benutzern den sicheren Zugriff auf Ihre Netzwerkressourcen zu ermöglichen.

Ihre Mitarbeiter, Partner und Kunden benötigen lediglich einen unterstützten Webbrowser und eine Internetverbindung für den Zugriff auf die intuitive Startseite der Appliance. Über diese Seite können Secure Access 700-Benutzer ihre Remotesitzung verwalten.

Die Installation, Konfiguration und Verwaltung einer SSL VPN-Appliance ist unkompliziert. Sie können die Netzwerkappliance entweder innerhalb weniger Minuten in einem Rack montieren, oder Sie verwenden die mitgelieferten Gummifüße, wenn Sie das Secure Access 700 auf einer Oberfläche aufstellen möchten. Sobald eine Verbindung mit Ihrem Netzwerk besteht, müssen Sie an der seriellen Konsole nur noch einige System- und Netzwerkeinstellungen eingeben, um auf die Webkonsole zuzugreifen. Die Webkonsole ist die Webschnittstelle, über die Sie die Appliance nach den Anforderungen Ihres Unternehmens konfigurieren und verwalten können. Die folgenden Features ermöglichen eine problemlose Bereitstellung und effiziente Wartung des Systems:

- Einfache Serverintegration – IVE-Appliances lassen sich in vorhandene Authentifizierungsserver (LDAP, RADIUS, NIS, Windows NT-Domäne, Active Directory und RSA ACE/Server) des Unternehmens integrieren. Sie müssen keine Änderungen an den internen Webservern, Dateiservern oder Netzwerken vornehmen.

- Zertifikatauthentifizierung – Schützt Anwendungen, ohne Änderungen an internen Ressourcen vorzunehmen. Geben Sie einfach eine digitale Zertifikatanforderung als Teil der Authentifizierungsrichtlinie des Bereichs an.

- Einfache Firewallrichtlinien – Von außen ist nur ein SSL-Zugriff auf das IVE erforderlich.

- Ressourcenzugriffssteuerung unter Verwendung des IVE-Zugriffsverwaltungssystems (Authentifizierungsbereiche, Benutzerrollen und Ressourcenrichtlinien)

- Zentralisierte Protokollierung auf Anwendungsebene, durch die Administrator- und Benutzeraktionen, Verbindungs-, Datei- und Webanforderungen sowie Systemfehler verfolgt werden.

- Systemsoftwareaktualisierungen über das Internet

- SNMP- und DMZ-Unterstützung

Zugriffsverwaltung – Übersicht

SSL VPN-Appliances ermöglichen es Ihnen, die Ressourcen Ihres Unternehmens mithilfe von Authentifizierungsrichtlinien, Benutzerprofilen und Ressourcenrichtlinien zu sichern. Mit diesen drei Kontrollstufen können Sie die Zugriffsverwaltung für das gesamte Unternehmen steuern. Sie können Sicherheitsanforderungen angeben, die Benutzer erfüllen müssen, um sich beim IVE anzumelden und auf IVE-Funktionen oder bestimmte -Ressourcen zugreifen zu können. Das IVE setzt die konfigurierten Richtlinien, Regeln und Einschränkungen sowie die Bedingungen durch, mit deren Hilfe die Benutzer daran gehindert werden, Verbindungen mit unautorisierten Ressourcen und Inhalten herzustellen oder diese herunterzuladen.

Weitere Informationen finden Sie unter:

- „Richtlinien, Regeln und Einschränkungen sowie Bedingungen“ auf Seite 38
- „Zugriff und Autorisierung – Flussdiagramm“ auf Seite 40
- „Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)“ auf Seite 44
- „Konfigurieren von Sicherheitsanforderungen“ auf Seite 46

Richtlinien, Regeln und Einschränkungen sowie Bedingungen

Das IVE ermöglicht es Ihnen, die Ressourcen Ihres Unternehmens mithilfe von Authentifizierungsrichtlinien, Benutzerprofilen und Ressourcenrichtlinien zu sichern. Mit diesen drei Zugriffsstufen können Sie den Zugriff von einer weitgefassten Ebene (z. B., wer sich am IVE anmelden kann) bis hinunter auf einer sehr enggefassten Ebene steuern (z. B., welche authentifizierten Benutzer auf ein bestimmtes URL oder eine bestimmte Datei zugreifen können).

Zugreifen auf Authentifizierungsbereiche

Der Zugriff auf Ressourcen beginnt im Authentifizierungsbereich. Als *Authentifizierungsbereich* wird eine Gruppierung von Authentifizierungsressourcen bezeichnet, einschließlich:

- **Eines Authentifizierungsservers**, durch den die Identität des Benutzers überprüft wird. Das IVE leitet die Anmeldeinformationen eines Benutzers von der Anmeldeseite an einen Authentifizierungsserver weiter. Weitere Informationen finden Sie unter „Authentifizierungsserver“ auf Seite 51.
- **Einer Authentifizierungsrichtlinie**, die die Sicherheitsanforderungen des Bereichs angibt, die erfüllt sein müssen, damit das IVE die Anmeldeinformationen eines Benutzers zur Überprüfung an einen Authentifizierungsserver weiterleitet. Weitere Informationen finden Sie unter „Authentifizierungsrichtlinien“ auf Seite 53.
- **Eines Verzeichnisservers**, das ist ein LDAP-Server, der dem IVE Benutzer- und Gruppeninformationen bereitstellt, mit denen das IVE Benutzer einer Benutzerrolle oder mehreren Benutzerrollen zuordnet. Weitere Informationen finden Sie unter „Verzeichnisserver“ auf Seite 53.

- **Rollenzuordnungsregeln**, diese geben die Bedingungen an, die ein Benutzer erfüllen muss, damit er vom IVE Rollen zugewiesen wird. Diese Bedingungen beruhen entweder auf den Benutzerinformationen, die der Verzeichnisserver des Bereichs zurückgibt, oder auf dem Benutzernamen des Benutzers. Weitere Informationen finden Sie unter „Rollenzuordnungsregeln“ auf Seite 53.

Einer IVE-Anmeldeseite ist mindestens ein Authentifizierungsbereich zugeordnet. Wenn mehrere Bereiche für eine Anmeldeseite vorhanden sind, muss der Benutzer vor der Übermittlung der Anmeldeinformationen einen Bereich angeben. Wenn der Benutzer die Anmeldeinformationen übermittelt hat, überprüft das IVE die Authentifizierungsrichtlinie des gewählten Bereichs. Der Benutzer muss die für die Authentifizierungsrichtlinien des Bereichs angegebenen Sicherheitsanforderungen erfüllen, andernfalls leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter.

Auf Bereichsebene können Sie Sicherheitsanforderungen angeben, die auf verschiedenen Elementen basieren, wie z. B. auf der IP-Quelladresse des Benutzers oder dem Besitz eines clientseitigen Zertifikats. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie für den Bereich erfüllt, leitet das IVE die Anmeldeinformationen des Benutzers an den entsprechenden Authentifizierungsserver weiter. Wenn der Benutzer durch den Server authentifiziert wurde, wertet das IVE die Rollenzuordnungsregeln für den Bereich aus und ermittelt, welche Rollen dem Benutzer zugeordnet werden.

Weitere Informationen finden Sie unter „Authentifizierungsbereiche – Übersicht“ auf Seite 51.

Zugreifen auf Benutzerrollen

Eine *Rolle* ist eine definierte Einheit, die die IVE-Sitzungseigenschaften für die Benutzer angibt, die der Rolle zugeordnet sind. Zu diesen Sitzungseigenschaften gehören Informationen wie beispielsweise Sitzungszeitbegrenzungen und aktivierte Zugriffsfunktionen. Die Rollenkonfiguration bildet die zweite Ebene der Ressourcenzugriffssteuerung. Eine Rolle gibt nicht nur die Zugriffsmechanismen an, die einem Benutzer zur Verfügung stehen, sondern auch Beschränkungen, denen Benutzer entsprechen müssen, um einer Rolle zugeordnet werden zu können. Der Benutzer muss diese Sicherheitsanforderungen erfüllen, andernfalls ordnet ihn das IVE keiner Rolle zu.

Auf Bereichsebene können Sie Sicherheitsanforderungen auf der Grundlage von Elementen angeben, z. B. basierend auf der IP-Quelladresse des Benutzers oder basierend auf dem Besitz eines clientseitigen Zertifikats. Wenn der Benutzer die Anforderungen erfüllt, die von einer Rollenzuordnungsregel oder den Einschränkungen einer Rolle angegeben sind, ordnet das IVE den Benutzer einer Rolle zu. Wenn ein Benutzer eine Anforderung an die für die Rolle verfügbaren Backend-Ressourcen sendet, wertet das IVE die entsprechenden Ressourcenrichtlinien für die Zugriffsfunktion aus.

Beachten Sie, dass Sie Sicherheitsanforderungen für eine Rolle festlegen, indem Sie in der Rollendefinition Beschränkungen definieren. Das IVE wertet die angegebenen Anforderungen aus. Dies gewährleistet, dass nur Benutzer einer Rolle zugeordnet werden, die die Anforderungen erfüllen.

Weitere Informationen finden Sie unter „Benutzerrollen – Übersicht“ auf Seite 56.

Zugreifen auf Ressourcenrichtlinien

Eine *Ressourcenrichtlinie* ist eine Reihe von Ressourcennamen (beispielsweise Hostnamen und die Kombination aus IP-Adresse und Netzmaske), für die Sie den Zugriff zulassen oder verweigern. Eine Ressourcenrichtlinie bildet die dritte Ebene der Ressourcenzugriffssteuerung. Eine Rolle gewährt den Zugriff auf bestimmte Zugriffsfunktionen und Ressourcen, wohingegen eine Ressourcenrichtlinie den Benutzerzugriff auf eine bestimmte Ressource steuert. Mithilfe dieser Richtlinien können sogar Bedingungen angegeben werden, die, sofern erfüllt, den Benutzerzugriff auf eine Serverfreigabe oder Datei verweigern oder gewähren. Derartige Bedingungen können auf den von Ihnen angegebenen Sicherheitsanforderungen basieren. Der Benutzer muss diese Sicherheitsanforderungen erfüllen, andernfalls wird die Benutzeranforderung vom IVE nicht verarbeitet.

Auf Ressourcenebene können Sie Sicherheitsanforderungen auf der Grundlage von Elementen angeben, wie z. B. auf der Grundlage der IP-Quelladresse des Benutzers oder auf der Grundlage des Besitzes eines clientseitigen Zertifikats. Wenn der Benutzer die Anforderungen erfüllt, die in den Bedingungen einer Ressourcenrichtlinie angegeben sind, verweigert oder gewährt das IVE den Zugriff auf die angeforderte Ressource.

Weitere Informationen finden Sie unter „Ressourcenrichtlinien – Übersicht“ auf Seite 59.

Zugriff und Autorisierung – Flussdiagramm

In diesem Flussdiagramm werden die Transaktionen zwischen einem Benutzer und der IVE sowie zwischen der IVE und einem Authentifizierungsbereich dargestellt. Das Flussdiagramm beginnt an dem Punkt, an dem ein Benutzer in der IVE-Anmeldungsseite einen URL eingibt, und endet damit, dass der Benutzer die Benutzersitzung eigenständig beendet.

Abbildung 19: IVE authentifiziert Benutzer für Bereich und primären Server

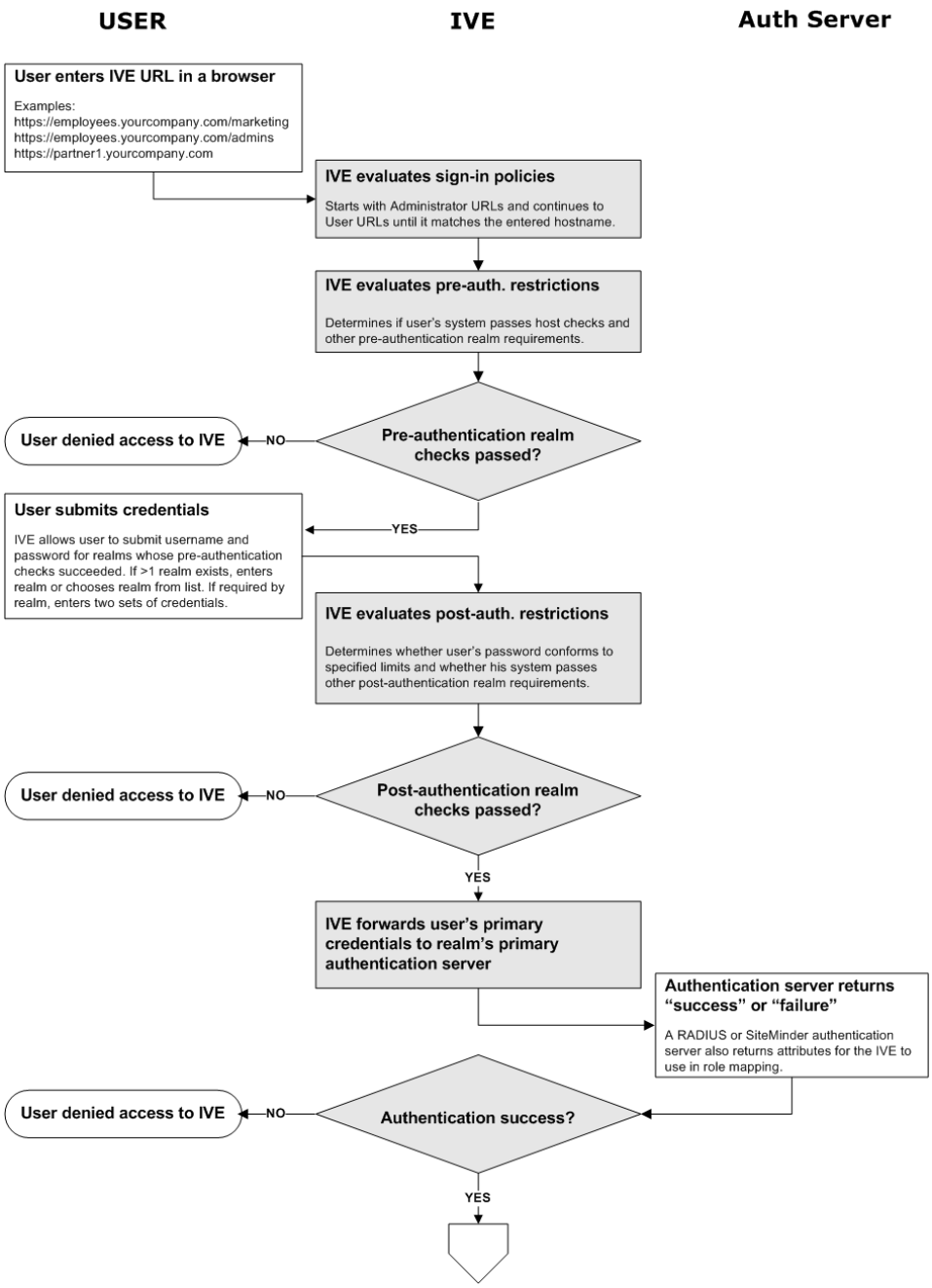

USER
IVE
Auth Server
User enters IVE URL in a browser
Examples:
https://employees.yourcompany.com/marketing
https://employees.yourcompany.com/admins
https://partner1.yourcompany.com
IVE evaluates sign-in policies
Starts with Administrator URLs and continues to User URLs until it matches the entered hostname.
IVE evaluates pre-auth. restrictions
Determines if user's system passes host checks and other pre-authentication realm requirements.
Pre-authentication realm checks passed?
NO
User denied access to IVE
YES
User submits credentials
IVE allows user to submit username and password for realms whose pre-authentication checks succeeded. If >1 realm exists, enters realm or chooses realm from list. If required by realm, enters two sets of credentials.
IVE evaluates post-auth. restrictions
Determines whether user's password conforms to specified limits and whether his system passes other post-authentication realm requirements.
Post-authentication realm checks passed?
NO
User denied access to IVE
YES
IVE forwards user's primary credentials to realm's primary authentication server
Authentication server returns "success" or "failure"
A RADIUS or SiteMinder authentication server also returns attributes for the IVE to use in role mapping.
Authentication success?
NO
User denied access to IVE
YES

Abbildung 20: IVE autorisiert Benutzer und authentifiziert für sekundären Server

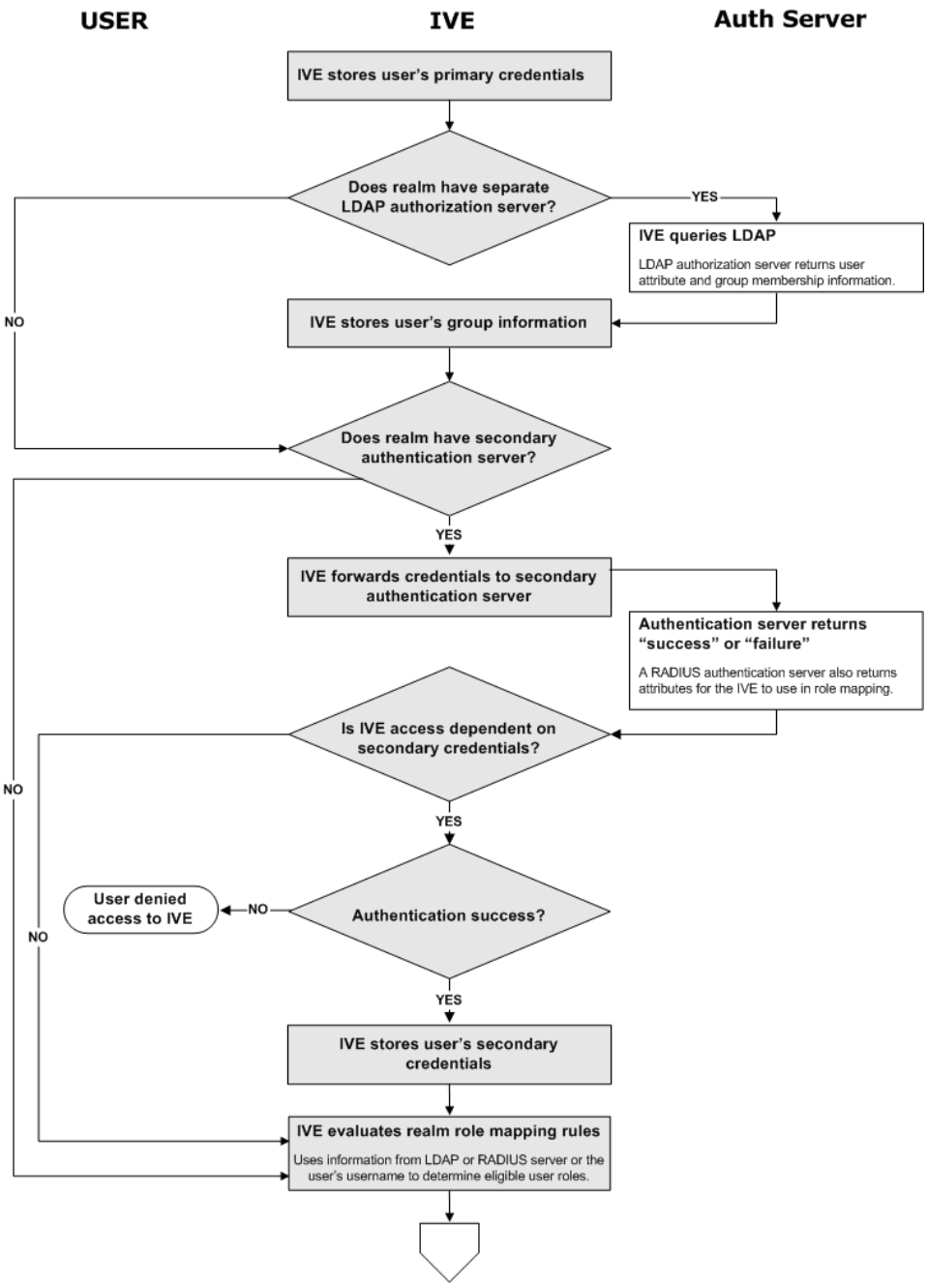
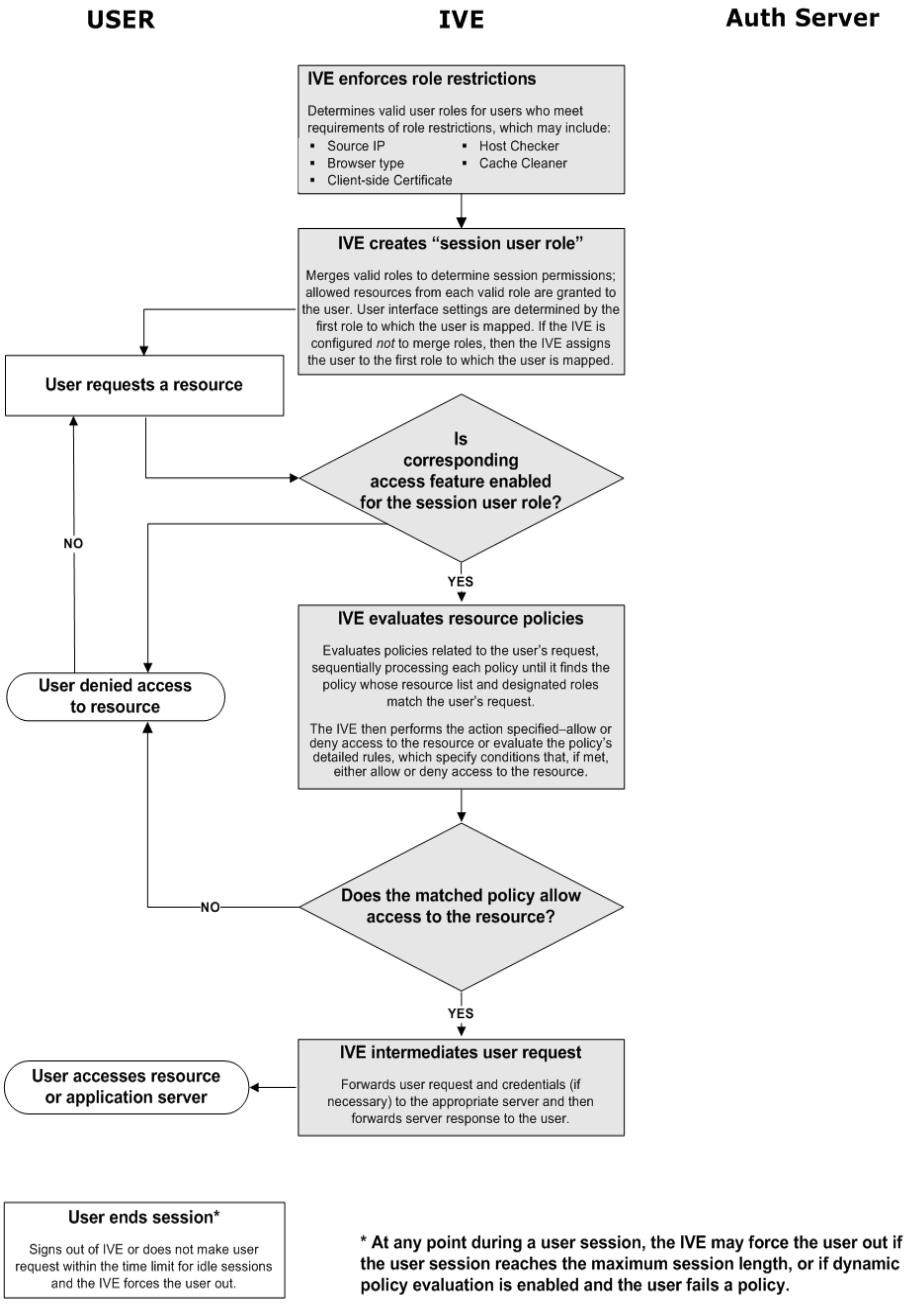

USER
IVE
Auth Server
IVE stores user's primary credentials
Does realm have separate LDAP authorization server?
YES
IVE queries LDAP
LDAP authorization server returns user attribute and group membership information.
NO
IVE stores user's group information
Does realm have secondary authentication server?
YES
IVE forwards credentials to secondary authentication server
Authentication server returns "success" or "failure"
A RADIUS authentication server also returns attributes for the IVE to use in role mapping.
Is IVE access dependent on secondary credentials?
NO
YES
User denied access to IVE
NO
Authentication success?
NO
YES
IVE stores user's secondary credentials
IVE evaluates realm role mapping rules
Uses information from LDAP or RADIUS server or the user's username to determine eligible user roles.

Abbildung 21: IVE ordnet Benutzer mehreren Rollen zu und wertet Ressourcenrichtlinien aus

Wenn Sie die dynamische Richtlinienauswertung aktivieren, wiederholen sich die im folgenden Flussdiagramm dargestellten Transaktionen. (Weitere Informationen finden Sie unter „Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)“ auf Seite 44.)


USER
IVE
Auth Server
IVE enforces role restrictions
Determines valid user roles for users who meet requirements of role restrictions, which may include:
Source IP
Browser type
Client-side Certificate
Host Checker
Cache Cleaner
IVE creates "session user role"
Merges valid roles to determine session permissions; allowed resources from each valid role are granted to the user. User interface settings are determined by the first role to which the user is mapped. If the IVE is configured not to merge roles, then the IVE assigns the user to the first role to which the user is mapped.
User requests a resource
Is corresponding access feature enabled for the session user role?
NO
YES
IVE evaluates resource policies
Evaluates policies related to the user's request, sequentially processing each policy until it finds the policy whose resource list and designated roles match the user's request.
The IVE then performs the action specified–allow or deny access to the resource or evaluate the policy's detailed rules, which specify conditions that, if met, either allow or deny access to the resource.
User denied access to resource
Does the matched policy allow access to the resource?
NO
YES
IVE intermediates user request
Forwards user request and credentials (if necessary) to the appropriate server and then forwards server response to the user.
User accesses resource or application server
User ends session*
Signs out of IVE or does not make user request within the time limit for idle sessions and the IVE forces the user out.
* At any point during a user session, the IVE may force the user out if the user session reaches the maximum session length, or if dynamic policy evaluation is enabled and the user fails a policy.

Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)

Die dynamische Richtlinienauswertung ermöglicht die automatische oder manuelle Aktualisierung der zugewiesenen Rollen von Benutzern durch Auswertung der Authentifizierungsrichtlinie, der Rollenzuordnungen, Rolleneinschränkungen und Ressourcenrichtlinien eines Bereichs.

Wenn Sie die dynamische Richtlinienauswertung nicht verwenden, wertet das IVE Richtlinien und Rollen *nur* bei den folgenden Ereignissen aus:

- Wenn der Benutzer das erste Mal auf die IVE-Anmeldeseite zugreifen möchte, wertet das IVE die Host Checker-Richtlinien (falls vorhanden) für einen Bereich aus.
- Unmittelbar nach der erstmaligen Authentifizierung des Benutzers wertet das IVE die Bereichseinschränkungen des Benutzers in der Authentifizierungsrichtlinie, in den Rollenzuordnungsregeln und Rolleneinschränkungen aus.
- Jedes Mal, wenn der Benutzer eine Ressource anfordert, wertet das IVE Ressourcenrichtlinien aus.
- Jedes Mal, wenn sich der Host Checker-Status des Computers ändert, wertet das IVE die Host Checker-Richtlinien (falls vorhanden) für eine Rolle aus.

Wenn Sie die dynamische Richtlinienauswertung nicht verwenden und Änderungen an einer Authentifizierungsrichtlinie, an Rollenzuordnungsregeln, Rolleneinschränkungen oder Ressourcenrichtlinien vornehmen, setzt das IVE diese Änderungen nur durch, wenn die oben beschriebenen Ereignisse auftreten.

Sie können die dynamische Richtlinienauswertung folgendermaßen verwenden:

- **Alle angemeldeten Benutzer in einem Bereich auswerten** – Sie können die Rollen aller derzeit angemeldeten Benutzer eines Bereichs automatisch oder manuell über die Registerkarte **General** der Seite **Administrators > Authentication >** *Ausgewählter Bereich* oder **Users > Authentication >** *Ausgewählter Bereich* aktualisieren. Sie können das IVE eine dynamische Richtlinienauswertung auf Bereichsebene folgendermaßen ausführen lassen:
  - **Mit einem automatischen Timer** – Legen Sie durch ein Aktualisierungsintervall fest, wie oft das IVE eine automatische Richtlinienauswertung aller derzeit angemeldeten Bereichsbenutzer ausführt (z. B. alle 30 Minuten). Bei Verwendung des Aktualisierungsintervalls können Sie auch die IVE-Leistung feiner abstimmen, indem Sie angeben, ob Rollen und Ressourcenrichtlinien sowie die Authentifizierungsrichtlinie, die Rollenzuordnungsregeln und Rolleneinschränkungen aktualisiert werden sollen oder nicht.

- **Nach Bedarf** – Sie können die Authentifizierungsrichtlinie, die Rollenzuordnungsregeln, Rolleneinschränkungen und Ressourcenrichtlinien aller derzeit angemeldeten Bereichsbenutzer jederzeit manuell auswerten. Diese Vorgehensweise ist besonders dann von Vorteil, wenn Sie Änderungen an einer Authentifizierungsrichtlinie, an Rollenzuordnungsregeln, Rolleneinschränkungen oder Ressourcenrichtlinien vornehmen möchten, und die Rollen der Benutzer dieses Bereichs sofort aktualisiert werden sollen.

Weitere Informationen über Richtlinienauswertung auf Bereichsebene finden Sie unter „Registerkarte „General““ auf Seite 257.

- **Alle angemeldeten Benutzer in allen Bereichen auswerten** – Sie können die Rollen aller derzeit angemeldeten Benutzer aller Bereiche jederzeit manuell auf der Registerkarte **Active Users** der Seite **System > Status > Active Users** aktualisieren. Informationen hierzu finden Sie unter „Registerkarte „Active Users““ auf Seite 156.

- **Einzelne Benutzer auswerten** – Sie können die Rollen einzelner Benutzer automatisch aktualisieren, indem Sie auf der Seite **Signing In > End Point > Host Checker** die dynamische Richtlinienauswertung für Host Checker aktivieren. Host Checker kann das IVE veranlassen, bei jeder Änderung des Host Checker-Status eines Benutzers Ressourcenrichtlinien auszuwerten. (Wenn die dynamische Richtlinienauswertung für Host Checker nicht aktiviert ist, wertet das IVE zwar keine Ressourcenrichtlinien aus, die Authentifizierungsrichtlinie, Rollenzuordnungsregeln und Rolleneinschränkungen werden dennoch bei jeder Änderung des Host Checker-Status eines Benutzers ausgewertet.) Weitere Informationen finden Sie unter „Registerkarte „Host Checker““ auf Seite 206.

Während der dynamischen Richtlinienauswertung wertet das IVE die folgenden Typen von Ressourcenrichtlinien aus:

- Network Connect
- Telnet/SSH
- Java Access
- Codesignatur (für Java-Applet)

HINWEIS: Das IVE wertet Web- und Files-Ressourcenrichtlinien immer aus, wenn der Benutzer eine Ressource anfordert. Eine dynamische Auswertung ist für diese Richtlinien daher nicht erforderlich. Das IVE verwendet die dynamische Richtlinienauswertung nicht für Meetings- und Email Client-Ressourcenrichtlinien.

Stellt das IVE nach einer dynamischen Richtlinienauswertung fest, dass ein Benutzer die Sicherheitsanforderungen einer Richtlinie oder Rolle nicht mehr erfüllt, beendet das IVE unverzüglich die Verbindung zum Benutzer. Das Schließen einer TCP-Verbindung oder Anwendungsverbindung oder das Beenden einer Benutzersitzung für Network Connect, Secure Application Manager, Terminal oder Telnet/SSH wird möglicherweise angezeigt. Der Benutzer muss die erforderlichen Schritte unternehmen, um die Sicherheitsanforderungen der Richtlinie oder Rolle zu erfüllen, und sich dann erneut am IVE anmelden.

Das IVE protokolliert Informationen über die Richtlinienauswertung und Rollen- oder Zugriffsänderungen im Ereignisprotokoll.

Konfigurieren von Sicherheitsanforderungen

Mit dem IVE können Sicherheitsanforderungen für Administratoren und Benutzer ganz einfach über die in den folgenden Abschnitten beschriebenen Optionen und Funktionen angegeben werden:

- „Quell-IP-Zugriffseinschränkungen“ auf Seite 46
- „Browserzugriffseinschränkungen“ auf Seite 47
- „Zertifikatzugriffseinschränkungen“ auf Seite 48
- „Kennwortzugriffseinschränkungen“ auf Seite 49
- „Host Checker-Zugriffseinschränkungen“ auf Seite 50
- „Cache Cleaner-Zugriffseinschränkungen“ auf Seite 50

Quell-IP-Zugriffseinschränkungen

Sie können den Zugriff auf das IVE und die Ressourcen anhand der Quell-IP einschränken.

- **Wenn sich Administratoren oder Benutzer am IVE anmelden möchten** – Der Benutzer muss sich an einem Computer anmelden, dessen Kombination aus IP-Adresse und Netzmaske die angegebenen IP-Quelladressanforderungen für den ausgewählten Authentifizierungsbereich erfüllt. Verfügt der Benutzercomputer nicht über eine für den Bereich erforderliche Kombination aus IP-Adresse und Netzmaske, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und dem Benutzer wird der Zugriff auf das IVE verweigert.

  Um IP-Einschränkungen auf Bereichsebene zu implementieren, navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP

- **Wenn Administratoren oder Benutzer einer Rolle zugeordnet werden** – Der authentifizierte Benutzer muss sich von einem Computer aus anmelden, dessen Kombination aus IP-Adresse und Netzmaske den angegebenen IP-Quelladressanforderungen für jede der Rollen entspricht, denen das IVE den Benutzer zuordnet. Verfügt der Benutzercomputer nicht über eine Kombination aus IP-Adresse und Netzmaske, die für eine Rolle erforderlich ist, ordnet das IVE den Benutzer dieser Rolle nicht zu.

Um IP-Einschränkungen auf Rollenebene zu implementieren, navigieren Sie zu:

- Administrators > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
- Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Source IP
- Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
- Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Source IP

- **Wenn Benutzer eine Ressource anfordern** – Der authentifizierte, autorisierte Benutzer kann eine Ressourcenanforderung nur von einem Computer durchführen, dessen Kombination aus IP-Adresse und Netzmaske den im Zusammenhang mit der Benutzeranforderung angegebenen IP-Quelladressanforderungen für die Ressourcenrichtlinie entspricht. Verfügt der Benutzercomputer nicht über die für eine Ressource erforderliche Kombination aus IP-Adresse und Netzmaske, gewährt das IVE dem Benutzer keinen Zugriff auf die Ressource.

  Um IP-Einschränkungen auf Ressourcenrichtlinienebene zu implementieren, navigieren Sie zu: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Browserzugriffseinschränkungen

Sie können den Zugriff auf das IVE und auf Ressourcen anhand des Browsertyps einschränken.

- **Wenn sich Administratoren oder Benutzer am IVE anmelden möchten** – Der Benutzer muss sich über einen Browser anmelden, dessen Benutzer-Agent-Zeichenfolge dem für den ausgewählten Authentifizierungsbereich angegebenen Zeichenfolgenmuster entspricht. Wenn die Benutzer-Agent-Zeichenfolge des Browsers für den Bereich zulässig ist, leitet das IVE die Anmeldeinformationen an den Authentifizierungsserver weiter. Wenn die Benutzer-Agent-Zeichenfolge des Browsers für den Bereich nicht zulässig ist, leitet das IVE die Anmeldeinformationen nicht an den Authentifizierungsserver weiter.

  Um Browsereinschränkungen auf Bereichsebene zu implementieren, navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser

- **Wenn Administratoren oder Benutzer einer Rolle zugeordnet werden** – Der authentifizierte Benutzer muss sich über einen Browser anmelden, dessen Benutzer-Agent-Zeichenfolge den jeweils angegebenen Zeichenfolgenmustern für die einzelnen Rollen entspricht, denen der Benutzer durch das IVE zugeordnet werden kann. Wenn die Benutzer-Agent-Zeichenfolge nicht den Zulassungsanforderungen für eine Rolle entspricht, ordnet das IVE den Benutzer dieser Rolle nicht zu.

  Um Browsereinschränkungen auf Rollenebene zu implementieren, navigieren Sie zu:

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Browser
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Browser

- **Wenn Benutzer eine Ressource anfordern** – Der authentifizierte, autorisierte Benutzer kann eine Ressourcenanforderung nur über einen Browser durchführen, dessen Benutzer-Agent-Zeichenfolge den im Zusammenhang mit der Benutzeranforderung angegebenen Zulassungsanforderungen für die Ressourcenrichtlinie entspricht. Wenn die Benutzer-Agent-Zeichenfolge nicht den Zulassungsanforderungen für eine Ressource entspricht, verweigert das IVE dem Benutzer den Zugriff auf die Ressource.

  Um Browsereinschränkungen auf Ressourcenrichtlinienebene zu implementieren, navigieren Sie zu: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Zertifikatzugriffseinschränkungen

Wenn Sie im IVE über die Seite **System > Configuration > Certificates > Trusted Client CAs** der Webkonsole ein clientseitiges Zertifikat installieren, können Sie den Zugriff auf das IVE und auf Ressourcen durch die Anforderung clientseitiger Zertifikate einschränken.

- **Wenn sich Administratoren oder Benutzer am IVE anmelden möchten** – Der Benutzer kann sich nur an einem Computer anmelden, der das angegebene clientseitige Zertifikat besitzt (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare). Wenn der Benutzercomputer nicht über die für den Bereich erforderlichen Zertifikatinformationen verfügt, kann der Benutzer auf die Anmeldeseite zugreifen, doch sobald vom IVE festgestellt wird, dass der Benutzerbrowser das Zertifikat nicht besitzt, werden die Anmeldeinformationen des Benutzers vom IVE nicht an den Authentifizierungsserver übermittelt, sodass der Benutzer nicht auf die Funktionen des IVE zugreifen kann.

  Um Zertifikateinschränkungen auf Bereichsebene zu implementieren, navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate

- Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate

- **Wenn Administratoren oder Benutzer einer Rolle zugeordnet werden** – Der authentifizierte Benutzer muss sich an einem Computer anmelden, der die angegebenen Anforderungen des clientseitigen Zertifikats (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare) für jede der Rollen erfüllt, der das IVE den Benutzer zuordnet. Besitzt der Benutzercomputer nicht die Zertifikatinformationen, die für eine Rolle erforderlich sind, ordnet das IVE den Benutzer dieser Rolle nicht zu.

  Um Zertifikateinschränkungen auf Rollenebene zu implementieren, navigieren Sie zu:

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Certificate

  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*

  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Certificate

- **Wenn Benutzer eine Ressource anfordern** – Der authentifizierte, autorisierte Benutzer muss eine Ressourcenanforderung von einem Computer ausführen, der die angegebenen Anforderungen des clientseitigen Zertifikats (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare) für die Ressourcenrichtlinie erfüllt, die für die Benutzeranforderung angegeben wurde. Besitzt der Benutzercomputer nicht die Zertifikatinformationen, die für eine Ressource erforderlich sind, verweigert das IVE dem Benutzer den Zugriff auf die Ressource.

  Um Zertifikateinschränkungen auf Ressourcenrichtlinienebene zu implementieren, navigieren Sie zu: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Kennwortzugriffseinschränkungen

Sie können den Zugriff auf das IVE und auf Ressourcen anhand der Kennwortlänge einschränken.

- **Wenn sich Administratoren oder Benutzer am IVE anmelden möchten** – Der Benutzer muss ein Kennwort eingeben, dessen Länge die für den Bereich angegebene Anforderung für die Mindestkennwortlänge erfüllt. Beachten Sie, dass die Datensätze für lokale Benutzer und Administratoren auf dem IVE-Authentifizierungsserver gespeichert werden. Auf diesem Server müssen Kennwörter mindestens 6 Zeichen lang sein, unabhängig von dem Wert, der für die Authentifizierungsrichtlinie des Bereichs angegeben wurde.

  Um Kennworteinschränkungen auf Bereichsebene zu implementieren, navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password

- Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password

Host Checker-Zugriffseinschränkungen

Weitere Informationen über die auf dem Host Checker-Status basierende Einschränkung des Benutzerzugriffs auf das IVE, eine Rolle oder eine Ressource finden Sie unter „Implementieren von Host Checker-Richtlinien“ auf Seite 81.

Cache Cleaner-Zugriffseinschränkungen

Weitere Informationen über die auf dem Cache Cleaner-Status basierende Einschränkung des Benutzerzugriffs auf das IVE, eine Rolle oder eine Ressource finden Sie unter „Cache Cleaner implementieren“ auf Seite 88.

Authentifizierungsbereiche – Übersicht

Als *Authentifizierungsbereich* wird eine Gruppierung von Authentifizierungsressourcen bezeichnet, einschließlich:

- **Eines Authentifizierungsservers**, durch den die Identität des Benutzers überprüft wird. Das IVE leitet die Anmeldeinformationen eines Benutzers von der Anmeldeseite an einen Authentifizierungsserver weiter. Weitere Informationen finden Sie unter „Authentifizierungsserver“ auf Seite 51.
- **Einer Authentifizierungsrichtlinie**, die die Sicherheitsanforderungen des Bereichs angibt, die erfüllt sein müssen, damit das IVE die Anmeldeinformationen eines Benutzers zur Überprüfung an einen Authentifizierungsserver weiterleitet. Weitere Informationen finden Sie unter „Authentifizierungsrichtlinien“ auf Seite 53.
- **Eines Verzeichnisservers**, das ist ein LDAP-Server, der dem IVE Benutzer- und Gruppeninformationen bereitstellt, mit denen das IVE Benutzer einer Benutzerrolle oder mehreren Benutzerrollen zuordnet. Weitere Informationen finden Sie unter „Verzeichnisserver“ auf Seite 53.
- **Rollenzuordnungsregeln**, diese geben die Bedingungen an, die ein Benutzer erfüllen muss, damit er vom IVE Rollen zugewiesen wird. Diese Bedingungen beruhen entweder auf den Benutzerinformationen, die der Verzeichnisserver des Bereichs zurückgibt, oder auf dem Benutzernamen des Benutzers. Weitere Informationen finden Sie unter „Rollenzuordnungsregeln“ auf Seite 53.

Authentifizierungsserver

Bei einem ***Authentifizierungsserver*** handelt es sich um eine Datenbank, in der Anmeldeinformationen für Benutzer (Benutzername und Kennwort) und normalerweise Gruppeninformationen gespeichert werden. Wenn sich ein Benutzer am IVE anmeldet, gibt er einen Authentifizierungsbereich an, der einem Authentifizierungsserver zugeordnet ist. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie erfüllt, leitet das IVE die Anmeldeinformationen des Benutzers an den zugeordneten Authentifizierungsserver weiter. Der Authentifizierungsserver überprüft die Existenz und Identität der Benutzer. Anschließend sendet der Authentifizierungsserver die Bestätigung und, wenn der Server in dem Bereich auch als Verzeichnis-/Attributserver verwendet wird, auch die Gruppeninformationen des Benutzers oder andere Benutzerattributinformationen an das IVE. Das IVE ermittelt die Rollenzuordnungsregeln für den Bereich und die Benutzerrollen, denen ein Benutzer zugeordnet werden kann.

HINWEIS: Sie können einem Bereich auch einen zweiten Authentifizierungsserver zuordnen. Wenn Sie einen zweiten Authentifizierungsserver zuordnen, sendet das IVE die Benutzerinformationen vor dem Zuordnen des Benutzers zur Rolle an den zweiten Authentifizierungsserver.

Zum Angeben eines Authentifizierungsservers, der für einen Bereich verwendet werden kann, müssen Sie zunächst auf der Seite **Signing In > AAA Servers** eine Serverinstanz konfigurieren. Wenn Sie die Servereinstellungen speichern, wird der Servername (der der Instanz zugewiesene Name) auf der Registerkarte **General** des Bereichs in der Dropdownliste **Authentication** angezeigt. Es gibt zwei Möglichkeiten:

- **LDAP- oder Active Directory-Server** – Der Instanzenname wird auch in der Dropdownliste **Directory/Attribute** auf der Registerkarte **General** des Bereichs angezeigt. Sie können den gleichen LDAP- oder Active Directory-Server sowohl für die Authentifizierung als auch für die Autorisierung des Bereichs verwenden. Außerdem können Sie diese Server für die Autorisierung einer beliebigen Anzahl von Bereichen verwenden, die unterschiedliche Authentifizierungsserver verwenden.

- **RADIUS-Server** – Der Instanzenname wird auch in der Dropdownliste **Accounting** auf der Registerkarte **General** des Bereichs angezeigt. Sie können den gleichen RADIUS-Server sowohl für die Authentifizierung als auch für die Kontoverwaltung des Bereichs verwenden. Außerdem können Sie diese Server für die Verwaltung einer beliebigen Anzahl von Bereichen verwenden, die unterschiedliche Authentifizierungsserver verwenden.

Das Secure Access 700 unterstützt die gängigen Authentifizierungsserver, z. B. Windows NT-Domäne, Active Directory, RADIUS, LDAP, NIS und RSA ACE/Server. Sie können eine oder mehrere lokale Datenbanken für vom IVE authentifizierte Benutzer erstellen. Eine Übersicht über Server und Informationen zur Konfiguration finden Sie unter:

- „Konfigurieren einer ACE/Serverinstanz“ auf Seite 234
- „Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz“ auf Seite 245
- „Konfigurieren einer Instanz eines anonymen Servers“ auf Seite 250
- „Konfigurieren einer Zertifikatserverinstanz“ auf Seite 252
- „Konfigurieren einer LDAP-Serverinstanz“ auf Seite 230
- „Konfigurieren einer lokalen Authentifizierungsserverinstanz“ auf Seite 225
- „Konfigurieren einer NIS-Serverinstanz“ auf Seite 233
- „Konfigurieren einer RADIUS-Serverinstanz“ auf Seite 238

HINWEIS: Ein Authentifizierungsserver muss eine Verbindung mit dem IVE herstellen können. Wenn ein Authentifizierungsserver wie RSA ACE/Server keine IP-Adressen für die Agentenhosts verwendet, muss er den IVE-Hostnamen über einen DNS-Eintrag oder einen Eintrag in der eigenen Hostdatei auflösen können.

Authentifizierungsrichtlinien

Eine ***Authentifizierungsrichtlinie*** besteht aus einer Reihe von Regeln für einen Aspekt der Zugriffsverwaltung, die steuern, ob dem Benutzer eine Anmeldeseite für den Bereich angezeigt wird. Eine Authentifizierungsrichtlinie ist Bestandteil der Konfiguration eines Authentifizierungsbereichs. Sie gibt die Regeln für das IVE an, die vor dem Anzeigen einer Anmeldeseite berücksichtigt werden müssen. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie für den Bereich erfüllt, zeigt das IVE dem Benutzer die Anmeldeseite an und leitet die Anmeldeinformationen des Benutzers an den entsprechenden Authentifizierungsserver weiter. Wenn der Benutzer durch den Server authentifiziert wird, beginnt das IVE mit der Rollenauswertung.

Verzeichnisserver

Ein *Verzeichnisserver* ist eine Datenbank, in der Benutzer- und normalerweise Gruppeninformationen gespeichert werden. Sie können einen Authentifizierungsbereich so konfigurieren, dass ein Verzeichnisserver Benutzer- oder Gruppeninformationen abruft, die in Rollenzuordnungsregeln und Ressourcenrichtlinien verwendet werden. Gegenwärtig unterstützt das IVE hierfür LDAP-Server; ein LDAP-Server kann daher zur Authentifizierung und Autorisierung verwendet werden. Sie müssen nur eine Serverinstanz definieren, dann wird der Name der LDAP-Serverinstanz in den Dropdownlisten **Authentication** und **Directory/Attribute** auf der Registerkarte **General** des Bereichs angezeigt. Sie können denselben Server für eine unbeschränkte Anzahl von Bereichen verwenden.

Neben einem LDAP-Server können Benutzerattribute auch mit einem RADIUS-Server abgerufen werden, um sie in Rollenzuordnungsregeln zu verwenden. Ein RADIUS-Serverinstanzenname wird jedoch im Gegensatz zu einer LDAP-Serverinstanz nicht in der Dropdownliste **Directory/Attribute** des Bereichs angezeigt. Um einen RADIUS-Server zum Abrufen von Benutzerinformationen zu verwenden, müssen Sie nur seinen Instanzennamen in der Liste **Authentication** auswählen; dann wählen Sie in der Liste **Directory/Attribute** die Option **Same as Above**. Anschließend konfigurieren Sie Rollenzuordnungsregeln, um Attribute des RADIUS-Servers zu verwenden, die in einer Attributliste auf der Seite **Role Mapping Rule** verfügbar sind, nachdem **Rule based on User attribute** ausgewählt wurde.

Weitere Informationen zum Angeben eines Verzeichnisservers finden Sie unter „Erstellen eines Authentifizierungsbereichs“ auf Seite 257. Weitere Informationen zum Angeben von LDAP- oder RADIUS-Attributen in Rollenzuordnungsregeln finden Sie unter „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 261.

Rollenzuordnungsregeln

Eine *Rollenzuordnungsregel* ist eine Anweisung, die in folgendem Format angegeben wird:

Wenn die angegebene Bedingung wahr|nicht wahr ist, dann ordne den Benutzer den ausgewählten Rollen zu.

Sie erstellen eine Rollenzuordnungsregel auf der Registerkarte **Role Mapping** eines Authentifizierungsbereichs. (Administratoren erstellen Rollenzuordnungsregeln auf der Registerkarte **Administrators > Authentication > [Bereich] > Role Mapping**. Benutzer erstellen Rollenzuordnungsregeln auf der Registerkarte **Users > Authentication > [Bereich] > Role Mapping**.) Wenn Sie auf dieser Registerkarte auf **New Rule** klicken, wird die Seite **Role Mapping Rule** angezeigt. Sie enthält einen integrierten Editor für die Definition von Regeln. Der Editor führt Sie durch die drei Schritte, die zum Erstellen einer Regel notwendig sind:

1. Geben Sie den Bedingungstyp an, auf dem die Regel beruhen soll. Folgende Optionen stehen zur Verfügung:
   - Benutzername
   - Zertifikat oder Zertifikatsattribut
   - Gruppenmitgliedschaft
2. Geben Sie die auszuwertende Bedingung an, die sich folgendermaßen zusammensetzt:
   a. Angeben von einem oder mehreren Benutzernamen, Benutzerattributen, Zertifikatsattributen oder Gruppen (LDAP) , die von dem in Schritt 1 ausgewählten Bedingungstyp abhängen.
   b. Angeben der Wertentsprechungen. Dies kann auch eine Liste von Benutzernamen, Benutzerattributswerten von einem RADIUS- oder LDAP-Server, clientseitigen Zertifikatswerten (statisch oder verglichen mit LDAP-Attributen) oder LDAP-Gruppen umfassen.
3. Geben Sie die Rollen an, die dem authentifizierten Benutzer zugewiesen werden sollen.

Das IVE stellt eine Liste aller *zulässigen Rollen* zusammen, denen ein Benutzer zugeordnet werden kann. Diese Rollen ergeben sich aus den Rollenzuordnungsregeln, denen ein Benutzer entspricht. Anschließend wertet das IVE die Definitionen der einzelnen Rollen aus, um festzustellen, ob der Benutzer Rolleneinschränkungen unterliegt. Das IVE erstellt anhand dieser Informationen eine Liste der *gültigen Rollen*, d. h. der Rollen, für die der Benutzer zusätzliche Anforderungen erfüllt. Abschließend führt das IVE entweder eine permissive Zusammenführung der gültigen Rollen durch oder zeigt dem Benutzer eine Liste gültiger Rollen an. Dies hängt von der Konfiguration ab, die auf der Registerkarte **Role Mapping** des Bereichs angegeben ist.

Weitere Informationen über Rollen finden Sie unter „Benutzerrollen – Übersicht“ auf Seite 56. Weitere Informationen über das Angeben von Rollenzuordnungsregeln finden Sie unter „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 261.

Anmelderichtlinien – Übersicht

Anmelderichtlinien definieren die URLs, die Benutzer und Administratoren für den Zugriff auf das IVE und die ihnen angezeigte Anmeldeseite verwenden können. Das IVE ist für Benutzer und Administratoren mit jeweils einer Anmelderichtlinie ausgestattet. Bei der Konfiguration dieser Richtlinien weisen Sie jeder Richtlinie die passenden Bereiche, Anmeldeseiten und URLs zu.

Um die Anmeldung beim IVE für alle Benutzer zuzulassen, müssen Sie der Benutzeranmelderichtlinie alle Benutzerauthentifizierungsbereiche hinzufügen. Sie können auch den Standard-URL ändern, den Benutzer für den Zugriff auf das IVE und die ihnen angezeigte Anmeldeseite verwenden.

Dieser Abschnitt enthält folgende Informationen zu Anmelderichtlinien:

- „Anmeldeseiten“ auf Seite 55
- „Aufgabenzusammenfassung: Konfigurieren von Anmelderichtlinien“ auf Seite 55

Anmeldeseiten

Eine *Anmeldeseite* legt die benutzerdefinierten Eigenschaften der Willkommensseite des Benutzers fest, wie etwa Begrüßungstext, Hilfetext, Logo, Kopf- und Fußzeile. Sie können die Standard-Anmeldeseite des IVE über die Seite **System > Signing In > Sign-in Pages** in der Webkonsole ändern.

Aufgabenzusammenfassung: Konfigurieren von Anmelderichtlinien

Gehen Sie zur Konfiguration von Anmelderichtlinien folgendermaßen vor:

1. Erstellen Sie einen Authentifizierungsbereich mit Hilfe einer der beiden folgenden Seiten in der Webkonsole: **Administrators > Authentication** oder **Users > Authentication**.
2. (Optional) Ändern Sie eine bereits bestehende Anmeldeseite oder erstellen Sie eine neue Seite über die Optionen der Seite **System > Signing In > Sign-in Pages** in der Webkonsole.
3. Bestimmen Sie eine Anmelderichtlinie, die eine Verknüpfung zwischen einem Bereich, einem Anmelde-URL und einer Anmeldeseite herstellt, unter Verwendung der Einstellungen auf der Seite **System > Signing In > Sign-in Policies** in der Webkonsole.

Benutzerrollen – Übersicht

Eine *Benutzerrolle* ist eine Einheit, die die folgenden Einstellungen festlegt: Parameter für Benutzersitzungen (Sitzungseinstellungen und -optionen), individuelle Einstellungen (benutzerdefinierte Einrichtung der Oberfläche und Lesezeichen) und aktivierte Zugriffsfunktionen (für Secure Access 700 ist Network Connect die einzige aktivierte Zugriffsfunktion). Eine Benutzerrolle steuert werden den Ressourcenzugriff noch gibt sie andere ressourcenbasierte Optionen für einzelne Anforderungen an. Zum Beispiel: Eine Benutzerrolle aktiviert die Zugriffsfunktion Network Connect, die einzelnen Ressourcen, auf die ein Benutzer zugreifen kann, werden jedoch von den getrennt konfigurierten „Network Connect Access Control“-Ressourcenrichtlinien definiert.

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

- „Rollenarten“ auf Seite 56
- „Rollenkomponenten“ auf Seite 56
- „Rollenauswertung“ auf Seite 57

Informationen zum Erstellen einer Benutzerrolle finden Sie unter „Konfigurieren der Seite „Roles““ auf Seite 276.

Rollenarten

Eine IVE unterstützt zwei Arten von Benutzerrollen:

- **Administrators** – Eine Administratorrolle ist eine Einheit, die die IVE-Verwaltungsfunktionen und -Sitzungseigenschaften für Administratoren angibt, die der Rolle zugeordnet sind. Sie können eine Administratorrolle anpassen, indem Sie Gruppen von IVE-Funktionen und Benutzerrollen auswählen, die Mitglieder der Administratorrolle anzeigen und verwalten dürfen. Sie erstellen und konfigurieren auf der Seite **Administrators > Delegation** der Webkonsole Administratorrollen.
- **Users** – Eine Benutzerrolle ist eine Einheit, die Parameter für Benutzersitzungen, individuelle Einstellungen und aktivierte Zugriffsfunktionen definiert. Durch Konfigurieren der IVE-Sitzungsoptionen, der benutzerdefinierten Einrichtung der Oberfläche, der Rolleneinschränkungen und Network Connect-Optionen können Sie eine Benutzerrolle anpassen. Sie erstellen und konfigurieren auf der Seite **Users > Roles** der Webkonsole Benutzerrollen.

Rollenkomponenten

Eine Benutzerrolle enthält die folgenden Informationen:

- **Role restrictions** – Die Verfügbarkeit der Rolle für die Benutzer beruht auf den Anforderungen bezüglich IP-Quelladresse, clientseitigem Zertifikat, Host Checker und Cache Cleaner, die erfüllt sein müssen, damit ein Benutzer einer Rolle zugewiesen wird.

- **Rollenbasierte Quell-IP-Aliase** – Auf Rollen basierender Benutzerzugriff auf Netzwerkgeräte hinter dem IVE. Wenn Sie den Verkehr basierend auf Rollen an bestimmte Sites senden möchten, können Sie für jede Rolle einen Quell-IP-Alias definieren.

- **Session parameters**– Sitzungseinstellungen, wie Zeitlimitwerte (Leerlaufzeit, Maximum, Erinnerung), Warnungen bei Zeitüberschreitung, Roamingsitzungen und permanente Sitzungsoptionen.

- **User interface options** – Individuelle Einstellungen, einschließlich Anmeldeseite, Kopf- und Fußzeile der Seiten sowie Anzeige der Browsing-Symbolleiste. Wenn der Benutzer mehreren Rollen zugeordnet ist, zeigt das IVE die Benutzeroberfläche entsprechend der ersten Rolle an, der der Benutzer zugeordnet wurde.

- **Network Connect-Settings** – Network Connect-Zugriffsfunktionen wie der Benutzerzugriff auf das lokale Subnetz.

Rollenauswertung

Das IVE-Rollenzuordnungsmodul bestimmt die *Sitzungsrolle* eines Benutzers bzw. kombinierte Berechtigungen, die für eine Benutzersitzung gültig sind. Dies geschieht wie folgt:

1. Das IVE beginnt die Rollenauswertung mit der ersten Regel auf der Registerkarte **Role Mapping** des Authentifizierungsbereichs, an dem sich der Benutzer erfolgreich anmeldet.

2. Das IVE ermittelt, ob der Benutzer die Bedingungen der Regel erfüllt. Wenn dies der Fall ist, führt das IVE Folgendes durch:

   a. Das IVE fügt die entsprechenden Rollen einer Liste von „zulässigen Rollen“ hinzu, die dem Benutzer zur Verfügung stehen.

   b. Das IVE berücksichtigt dabei, ob konfiguriert wurde, dass die Verarbeitung bei einem Treffer beendet werden soll (Option „Stop on Match“). Wenn dies der Fall ist, fährt das Modul mit Schritt 5 fort.

3. Das IVE wertet die nächste Regel auf der Registerkarte **Role Mapping** des Authentifizierungsbereichs gemäß des Vorgangs in Schritt 2 aus und wiederholt diesen Vorgang für jede weitere Regel. Wenn das IVE alle Rollenzuordnungsregeln auswertet, entsteht eine umfassende Liste möglicher Rollen.

4. Das IVE wertet die Definitionen aller Rollen in der Liste der zulässigen Rollen aus und überprüft, ob der Benutzer Rolleneinschränkungen unterliegt. Das IVE verwendet diese Informationen zum Erstellen einer Liste mit *gültigen Rollen*, deren Anforderungen vom Benutzer ebenfalls erfüllt werden.

   Wenn die Liste gültiger Rollen nur eine Rolle enthält, ordnet das IVE den Benutzer dieser Rolle zu. Andernfalls setzt das IVE die Auswertung fort.

5. Für Benutzer, die mehreren Rollen zugeordnet sind, wertet die IVE die Einstellung aus, die auf der Registerkarte **Role Mapping** angegeben ist.

   - **Merge settings for all assigned roles** – Wenn Sie diese Option auswählen, führt das IVE eine permissive Zusammenführung aller gültigen Benutzerrollen durch, um die Gesamtrolle (Netzrolle) für eine Benutzersitzung zu ermitteln.

   - **User must select from among assigned roles** – Wenn Sie diese Option aktivieren, zeigt das IVE für einen authentifizierten Benutzer eine Liste zulässiger Rollen an. Der Benutzer muss eine Rolle aus der Liste auswählen, und das IVE weist den Benutzer dann für die Dauer der Benutzersitzung dieser Rolle zu.

   - **User must select the sets of merged roles assigned by each rule** – Bei Auswahl dieser Option erhalten Sie vom IVE eine Liste mit möglichen Regeln für einen authentifizierten Benutzer (d. h. Regeln, deren Bedingungen der Benutzer erfüllt). Der Benutzer muss in der Liste eine Regel auswählen, und das IVE führt eine permissive Zusammenführung aller Rollen, die dieser Regel zugewiesen sind, aus.

HINWEIS: Bei Verwendung der automatischen (zeitgesteuerten) dynamischen oder der manuellen Richtlinienauswertung wiederholt das IVE den in diesem Abschnitt beschriebenen Rollenauswertungsvorgang. Weitere Informationen finden Sie unter „Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)“ auf Seite 44.

Richtlinien für permissive Zusammenführungen

Eine *permissive Zusammenführung* ist eine Zusammenführung mehrerer Rollen, die *aktivierte* Funktionen und Einstellungen anhand der folgenden Richtlinien kombiniert:

- Im Fall von Benutzeroberflächenoptionen wendet das IVE die Einstellungen an, die mit der ersten Rolle des Benutzers übereinstimmen.

- Bei Überschreitungen der Sitzungsdauer wendet das IVE den höchsten Wert aller Rollen auf die Benutzersitzung an.

- Ist die Funktion **Roaming Session** für mehrere Rollen aktiviert, führt das IVE die Netzmasken zusammen, um die Netzmaske für die Sitzung zu erweitern.

- Von der zusammengeführten Rolle wird für **HTTP Connection Timeout** auf der Seite **Roles > [Rolle] > Web > Options** der höchste Wert verwendet.

Ressourcenrichtlinien – Übersicht

Eine *Ressourcenrichtlinie* ist eine Systemregel, die Ressourcen und Aktionen für eine bestimmte Zugriffsfunktion angibt. (Der Secure Access 700 verwendet ein Zugriffsfeature – Network Connect.) Eine Ressource kann entweder ein Server oder eine Datei sein, auf die über eine IVE-Appliance zugegriffen werden kann. Mithilfe einer Aktion wird einer Ressource „erlaubt“ oder „verboten“, eine Funktion durchzuführen. Jede Zugriffsfunktion verfügt über mindestens einen Richtlinientyp, der die Antwort der IVE-Appliance auf eine Benutzeranforderung bestimmt. Sie können auch detaillierte Regeln für eine Ressourcenrichtlinie definieren, mit denen Sie zusätzliche Anforderungen für bestimmte Benutzeranforderungen auswerten können.

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

- „Typen von Ressourcenrichtlinien“ auf Seite 59
- „Bestandteile einer Ressourcenrichtlinie“ auf Seite 59
- „Auswerten von Ressourcenrichtlinien“ auf Seite 60

Typen von Ressourcenrichtlinien

Die Secure Access 700 Network Connect-Zugriffsfunktion verfügt über drei Arten von Ressourcenrichtlinien:

- **Network Connect Access Control** – Dieser Richtlinientyp steuert, mit welchen Ressourcen Benutzer über Network Connect eine Verbindung herstellen können.
- **IP Address Pools** – Dieser Richtlinientyp gibt einen IP-Pool an, aus dem die IVE-Appliance dem Clientprozess für eine Network Connect-Sitzung eine IP-Adresse zuweist.
- **Split Tunneling Network** – Dieser Richtlinientyp gibt die internen Netzwerke an, für die die IVE-Appliance den Datenverkehr regelt.

Bestandteile einer Ressourcenrichtlinie

Eine Ressourcenrichtlinie enthält die folgenden Informationen:

- **Ressourcen:** Eine Reihe von Ressourcennamen (Hostnamen oder Kombinationen aus IP-Adresse/Netzmaske), die die Ressourcen angeben, für die die Richtlinie gilt. Sie können eine Ressource mit einem Platzhalterpräfix angeben, das für einen Hostnamen steht. Die Standardressource für eine Richtlinie wird durch ein Sternchen (*) angegeben, d. h., die Richtlinie gilt für alle entsprechenden Ressourcen. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305.
- **Rollen:** Eine optionale Liste von Benutzerrollen, für die diese Richtlinie gilt. Standardmäßig gilt die Richtlinie für alle Rollen.

- **Aktion:** Die Aktion, die von einer IVE-Appliance durchgeführt wird, wenn ein Benutzer die Ressource entsprechend der Liste **Resource** anfordert. Eine Aktion kann angeben, ob der Zugriff auf eine Ressource erlaubt oder verboten ist oder bestimmte IP-Adressen zuweisen.

Auswerten von Ressourcenrichtlinien

Wenn eine IVE-Appliance eine Benutzeranforderung erhält, wertet es die dem Anforderungstyp entsprechenden Ressourcenrichtlinien aus. Beim Verarbeiten der Richtlinie, die der angeforderten Ressource entspricht, führt es die angegebene Aktion für die Anforderung aus. Diese Aktion ist auf der Registerkarte **General** der Richtlinie festgelegt.

Eine IVE-Appliance wertet eine Gruppe von Ressourcenrichtlinien für eine Zugriffsfunktion von oben nach unten aus, d. h., es startet mit der ersten Richtlinie und durchläuft dann die Liste, bis eine passende Richtlinie gefunden wird.

Ausführliche Regeln für Ressourcenrichtlinien

Mit den Zugriffsfunktionen für Web, Dateien, Telnet/SSH und Network Connect können Sie Ressourcenrichtlinien für einzelne Web-, Datei-, Anwendungs- und Telnet-Server angeben. Die Email Client-Zugriffsfunktion verfügt über eine global geltende Richtlinie. Für diese Richtlinie geben Sie Servereinstellungen an, die für alle Rollen verwendet werden, die diese Zugriffsfunktion unterstützen. Für alle anderen Zugriffsfunktionen können Sie eine beliebige Anzahl von Ressourcenrichtlinien angeben und für jede eine oder mehrere detaillierte Regeln definieren.

Eine *detaillierte Regel* ist eine Erweiterung einer Ressourcenrichtlinie, die Folgendes angeben kann:

- Zusätzliche[1] Ressourceninformationen (wie bestimmte Pfade, Dateien oder Dateitypen) für Ressourcen, die auf der Registerkarte **General** aufgelistet sind.
- Eine Aktion, die von der auf der Registerkarte **General** angegebenen Aktion abweicht (obwohl die Optionen die gleichen sind).
- Bedingungen, die erfüllt sein müssen, damit die detaillierte Regel angewendet werden kann.

In vielen Fällen ermöglicht die Basis-Ressourcenrichtlinie, d. h. die auf der Registerkarte **General** einer Ressourcenrichtlinie angegebenen Informationen, ausreichende Zugriffssteuerung für eine Ressource:

> Wenn ein Benutzer, der (definierte_Rollen) angehört, versucht, auf (definierte_Ressourcen) zuzugreifen, FÜHRE die angegebene (Ressourcen_Aktion) aus.

1. Beachten Sie, dass Sie die gleiche Ressourcenliste (wie auf der Registerkarte „General“) auch als detaillierte Regel angeben können, wenn deren einziger Zweck die Anwendung von Bedingungen auf eine Benutzeranforderung ist.

Sie können eine oder mehrere detaillierte Rollen für eine Richtlinie definieren, wenn Sie eine Aktion durchführen möchten, die auf einer Kombination anderer Informationen basiert, zu denen Folgende gehören können:

- Die Eigenschaften einer Ressource, beispielsweise Header, Inhaltstyp oder Dateityp
- Die Eigenschaften eines Benutzers, beispielsweise der Benutzername und die Rollen, denen er zugeordnet ist
- Die Eigenschaften einer Sitzung, beispielsweise die Quell-IP oder der Browsertyp eines Benutzers, ob der Benutzer die Hostprüfung oder Cachebereinigung ausführt, die Uhrzeit oder Zertifikatattribute

Mit detaillierten Regeln kann die Ressourcenzugriffssteuerung flexibler gestaltet werden, sodass bestehende Ressourcen- oder Berechtigungsinformationen zum Angeben anderer Anforderungen für andere Benutzer verwendet können, auf die die Basisressourcenrichtlinie angewendet wird.

Konfigurationsanweisungen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

Kapitel 3

Authentifizierung und Autorisierung

Alle auf der IVE-Plattform basierenden Produkte ermöglichen wie unter „Die IVE-Reihe“ auf Seite 31 beschrieben die Verwendung von Bereichen, Servern, Rollen und Ressourcenrichtlinien zur Verwaltung des Benutzerzugriffs auf das IVE und seine Funktionen. Darüber hinaus verfügt das IVE über die in den folgenden Abschnitten beschriebenen Authentifizierungs-, Autorisierungs- und Sicherheitsfunktionen.

Inhalt

- „Zertifikate – Übersicht“ auf Seite 65
- „Endpoint Defense – Übersicht“ auf Seite 74

Zertifikate – Übersicht

Die IVE sichert die über das Internet an Clients gesendete Daten mithilfe der PKI. *PKI* (Public Key Infrastructure) ist eine Sicherheitsmethode, bei der öffentliche und private Schlüssel zum Verschlüsseln und Entschlüsseln von Informationen verwendet werden. Diese Schlüssel werden über digitale Zertifikate aktiviert und gespeichert. Ein *digitales Zertifikat* ist eine verschlüsselte elektronische Datei, in der die Anmeldeinformationen eines Webservers oder Benutzers für Client-Server-Transaktionen festgelegt werden.

Ein IVE verwendet folgende Typen digitaler Zertifikate zum Festlegen von Anmeldeinformationen und zum Sichern von IVE-Sitzungstransaktionen:

- **IVE-Zertifikate** – Ein *IVE-Serverzertifikat* sichert den Netzwerkverkehr zu und von einer IVE-Appliance mithilfe bestimmter Elemente. Zu diesen Elementen zählen z. B. der Firmenname, eine Kopie des öffentlichen Schlüssels Ihres Unternehmens, die digitale Signatur der Zertifizierungsstelle (Certificate Authority, CA), die das Zertifikat ausgestellt hat, eine Seriennummer sowie ein Ablaufdatum. Weitere Informationen finden Sie unter „IVE Serverzertifikate“ auf Seite 66.

- **CAs vertrauter Clients** – Eine *Zertifizierungsstelle vertrauter Clients* ist ein von einer Zertifizierungsstelle oder Certificate Authority (CA) ausgestelltes clientseitiges Zertifikat zur Steuerung des Zugriffs auf Bereiche, Rollen und Ressourcenrichtlinien basierend auf Zertifikaten oder Zertifikatattributen. So können Sie beispielsweise festlegen, dass Benutzer ein gültiges clientseitiges Zertifikat mit dem auf „eigenefirma.com“ festgelegten Organisationseinheitsattribut vorlegen müssen, um sich am Authentifizierungsbereich „Users“ anmelden zu können. Weitere Informationen finden Sie unter „CAs vertrauter Clients“ auf Seite 67.

- **CAs eines vertrauten Servers** – Eine *Zertifizierungsstelle eines vertrauten Servers* ist das Zertifikat eines Webservers, dem Sie vertrauen können. Wenn Sie über eine Webbrowsing-Lizenz verfügen, können Sie auf dem IVE die Zertifizierungsstelle eines vertrauten Servers installieren und die Anmeldeinformationen für die Websites validieren, auf die die Benutzer über die IVE-Appliance zugreifen. Weitere Informationen finden Sie unter „CAs vertrauter Server“ auf Seite 71.

- **Codesignaturzertifikate** – Ein *Codesignaturzertifikat* (auch Appletzertifikat genannt) ist ein serverseitiges Zertifikat, das die vom IVE vermittelten Java-Applets neu signiert. Sie haben entweder die Möglichkeit, das auf einer IVE-Appliance vorinstallierte selbst signierte Codesignaturzertifikat zu verwenden oder ein eigenes Codesignaturzertifikat zu installieren. Weitere Informationen finden Sie unter „Codesignaturzertifikate“ auf Seite 72.

In einem grundlegenden IVE-Setup ist nur ein IVE-Zertifikat und ein Codesignaturzertifikat erforderlich. Die IVE-Appliance kann alle Java-Applets mit einem einzigen Codesignaturzertifikat neu signieren und alle weiteren PKI-basierten Interaktionen mit einem einzigen IVE-Serverzertifikat vermitteln. Sollten diese Basiszertifikate jedoch nicht Ihren Anforderungen entsprechen, können Sie mehrere Server- und Appletzertifikate auf einer IVE-Appliance installieren oder vertraute Zertifizierungsstellenzertifikate verwenden, um Benutzer zu überprüfen.

IVE Serverzertifikate

Ein IVE-Serverzertifikat sichert den Netzwerkverkehr zum und vom IVE mithilfe bestimmter Elemente. Zu diesen Elementen zählen z. B. der Firmenname, eine Kopie des öffentlichen Schlüssels Ihres Unternehmens, die digitale Signatur der Zertifizierungsstelle (Certificate Authority, CA), die das Zertifikat ausgestellt hat, eine Seriennummer sowie ein Ablaufdatum.

Wenn der Clientbrowser verschlüsselte Daten vom IVE empfängt, überprüft er zuerst, ob das Zertifikat des IVE gültig ist und ob der Benutzer der Zertifizierungsstelle vertraut, die das Zertifikat des IVE ausgestellt hat. Sofern der Benutzer nicht bereits angegeben hat, dass er dem IVE-Zertifikataussteller vertraut, wird er vom Webbrowser aufgefordert, das Zertifikat des IVE zu akzeptieren oder zu installieren.

Beim Initialisieren des IVE wird lokal ein temporäres, selbst signiertes digitales Zertifikat erstellt, mit dem die Benutzer sofort Ihr IVE verwenden können. Die Verschlüsselung für das während der Initialisierung erstellte selbst signierte Zertifikat ist zwar absolut sicher, für die Benutzer wird jedoch trotzdem bei jeder Anmeldung bei der IVE eine Sicherheitswarnung angezeigt, da das Zertifikat nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wird. Zu Produktionszwecken empfiehlt es sich, ein digitales Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle anzufordern.

Die IVE-Appliance unterstützt auch die Verwendung von Serverzwischenzertifikaten innerhalb einer Zertifikathierarchie, wie in „Serverzwischenzertifikate“ auf Seite 66 beschrieben.

Wenn Sie das in der IVE-Appliance automatisch erstellte selbst signierte Zertifikat nicht verwenden möchten, können Sie die Einstellungen auf der Seite **System > Configuration > Certificates > IVE Certificates** der Webkonsole verwenden, um:

- ein Stammzertifikat und den entsprechenden Privatschlüssel in die IVE-Appliance zu importieren.
- ein Serverzwischenzertifikat und den entsprechenden Privatschlüssel in die IVE-Appliance zu importieren. Weitere Informationen finden Sie unter „Serverzwischenzertifikate“ auf Seite 66.

Anweisungen hierfür finden Sie unter „Registerkarte „IVE Certificates““ auf Seite 166.

Serverzwischenzertifikate

Innerhalb einer *Zertifikathierarchie* werden Zwischenzertifikate von nur einem Stammzertifikat abgeleitet. Das Stammzertifikat wird von einer Stammzertifizierungsstelle (CA) ausgestellt und ist selbst-signiert. Jedes Zwischenzertifikat wird vom in der Kette übergeordneten Zertifikat ausgestellt.

Vergewissern Sie sich beim Sichern des Datenverkehrs mit verketteten Zertifikaten, dass das IVE und der Webbrowser die gesamte Zertifikatkette enthalten. Beispiel: Sie sichern den Verkehr mit einer Kette eines Verisign-Stammzertifikats. Wenn die Browser der Benutzer bereits mit Verisign-Stammzertifikaten ausgestattet sind, müssen Sie im IVE nur die untergeordneten Zertifikate der Kette installieren. Wenn die Benutzer daraufhin zum IVE navigieren, wird die Transaktion vom IVE durch

Anzeigen aller erforderlichen Zertifikate der Kette im Browser gesichert. (Das IVE erstellt die korrekten Verknüpfungen in der Kette mit der IssuerDN des Stammzertifikats.) Enthalten das IVE und der Browser nicht die gesamte Kette, erkennt der Browser des Benutzers das Zertifikat des IVE nicht bzw. er vertraut diesem nicht, da es nicht von einer vertrauten CA, sondern von einem anderen Zertifikat abstammt.

Informationen über verkettete Clientzertifikate finden Sie unter „Hierarchien von Clientzertifizierungsstellen“ auf Seite 68.

Installieren Sie Serverzwischenzertifikate über die Seite **System > Configuration > Certificates > IVE Certificates** der Webkonsole.

CAs vertrauter Clients

Eine *Zertifizierungsstelle eines vertrauten Clients* ist ein von einer Zertifizierungsstelle (CA) ausgestelltes clientseitiges Zertifikat. Damit Sie Client-Zertifizierungsstellenzertifikate verwenden können, müssen Sie die richtigen Zertifikate auf dem IVE installieren und aktivieren sowie die entsprechenden clientseitigen Zertifikate für die Webbrowser der Endbenutzer installieren. Beim Überprüfen der Benutzer mit Zertifizierungsstellenzertifikaten prüft das IVE, ob das Zertifikat abgelaufen oder beschädigt ist und ob es von einer vom IVE anerkannten Zertifizierungsstelle signiert wurde.

Weitere Informationen zur Konfiguration des IVE zum Einschränken des Benutzerzugriffs basierend auf Benutzer-Zertifikatswerten finden Sie unter „Zertifikatzugriffseinschränkungen“ auf Seite 48.

Das IVE unterstützt die Verwendung folgender zusätzlicher Features für Zertifizierungsstellenzertifikate:

- **Zertifikatserver** – Ein *Zertifikatserver* ist ein lokaler Authentifizierungsserver, mit dessen Hilfe Sie IVE-Benutzer lediglich auf der Grundlage ihrer Zertifikatattribute authentifizieren können, anstatt sie mithilfe eines Standardauthentifizierungsservers (z. B. LDAP oder RADIUS) zu authentifizieren. Außerdem sind spezifische Zertifikate oder Zertifikatattribute erforderlich. Weitere Informationen finden Sie unter „Konfigurieren einer Zertifikatserverinstanz“ auf Seite 252.

- **Zertifikathierarchien** – Innerhalb einer *Zertifikathierarchie* sind untergeordnete Zertifikate, die auch als Zwischenzertifikate bezeichnet werden, von nur einem Stammzertifikat abgeleitet und bilden eine Zertifikatkette. Wenn Sie auf dem IVE ein verkettetes Zertifikat installieren, überprüft die Appliance, ob die Kette gültig ist. Außerdem gestattet es dem Benutzer, sich mit dem untersten Zertifikat in der Kette zu authentifizieren. Weitere Informationen finden Sie unter „Hierarchien von Clientzertifizierungsstellen“ auf Seite 68.

- **Zertifikatsperrlisten** – Die *Zertifikatssperrung* ist ein Mechanismus, mit dem eine Zertifizierungsstelle die Gültigkeit eines Zertifikats vor dem Ablaufdatum aufhebt. Eine *Zertifikatsperrliste (Certificate Revocation List, CRL)* ist eine von einer Zertifizierungsstelle veröffentlichte Liste gesperrter Zertifikate. In Zertifikatsperrlisten enthält jeder Eintrag die Seriennummer des gesperrten Zertifikats, das Datum sowie den Grund der Zertifikatssperrung. Die Zertifizierungsstelle kann die Gültigkeit eines Zertifikats aus vielen verschiedenen Gründen aufheben, z. B. wenn ein Mitarbeiter, für den das

Zertifikat ausgestellt wurde, das Unternehmen verlassen hat, der private Schlüssel des Zertifikats gefährdet ist oder das clientseitige Zertifikat verloren gegangen ist oder gestohlen wurde. Nachdem die Zertifizierungsstelle ein Zertifikat gesperrt hat, kann das IVE Benutzern, die ein gesperrtes Zertifikat vorlegen, den Zugriff entsprechend verweigern. Weitere Informationen finden Sie unter „Zertifikatsperrlisten“ auf Seite 69.

Weitere Informationen zu Zertifikatüberprüfungen von Bereichen, Rollen und Ressourcenrichtlinien finden Sie unter „Zertifikateinschränkungen“ auf Seite 421.

Installieren Sie CAs vertrauter Clients über die Seite **System > Configuration > Certificates > Trusted Client CAs** in der Webkonsole. Anweisungen hierfür finden Sie unter „Hochladen von Zertifikaten der vertrauten Clientzertifizierungsstelle in das IVE“ auf Seite 171.

HINWEIS: Auf der Secure Access 700-Appliance können Sie lediglich ein Stammzertifikat auf dem IVE installieren und Benutzer unter Verwendung eines clientseitigen Zertifikats der Zertifizierungsstelle überprüfen.

Hierarchien von Clientzertifizierungsstellen

Innerhalb einer Zertifikathierarchie sind Zwischenzertifikate von nur einem Stammzertifikat abgeleitet. Das Stammzertifikat wird von einer Stammzertifizierungsstelle (CA) ausgestellt und ist selbst-signiert. Jedes Zwischenzertifikat wird vom in der Kette übergeordneten Zertifikat ausgestellt.

Zum Aktivieren der Authentifizierung in einer Umgebung mit verketteten Zertifikaten müssen Sie auf den Webbrowsern aller Benutzer die entsprechenden clientseitigen Zertifikate installieren und anschließend die entsprechenden CA-Zertifikate in das IVE laden.

HINWEIS: Sie können auf einer Secure Access 700-Appliance keine Kette installieren, deren Zertifikate von unterschiedlichen Zertifizierungsstellen ausgestellt werden. Die Zertifizierungsstelle, die das Zertifikat auf niedrigster Ebene in der Kette signiert, muss auch alle anderen Zertifikate in der Kette signieren.

Informationen über verkettete IVE-Serverzertifikate finden Sie unter „Serverzwischenzertifikate“ auf Seite 66.

Installieren Sie CAs vertrauter Clients über die Seite **System > Configuration > Certificates > Trusted Client CAs** in der Webkonsole. Sie müssen zum Hochladen der Zertifikatkette auf das IVE eine der folgenden Methoden anwenden:

- **Importieren der gesamten Zertifikatkette** – Beim Installieren einer Kette von Zertifikaten aus einer einzigen Datei importiert das IVE das Stammzertifikat sowie alle untergeordneten Zertifikate, deren übergeordnete Zertifikate sich in der Datei oder auf dem IVE befinden. Sie können die Zertifikate in beliebiger Reihenfolge in die Importdatei einschließen.

- **Importieren einzelner Zertifikate in absteigender Reihenfolge** – Beim Installieren einer Kette von Zertifikaten aus mehreren Dateien setzt das IVE voraus, dass Sie zuerst das Stammzertifikat und danach die restlichen verketteten Zertifikate in absteigender Reihenfolge installieren.

Wenn Sie verkettete Zertifikate mit Hilfe einer dieser Methoden installieren, verkettet das IVE die Zertifikate automatisch in der richtigen Reihenfolge und zeigt sie hierarchisch in der Webkonsole an.

Anweisungen hierfür finden Sie unter „Hochladen von Zertifikaten der vertrauten Clientzertifizierungsstelle in das IVE“ auf Seite 171.

Zertifikatsperrlisten

Eine *Zertifikatsperrliste (Certificate Revocation List; CRL)* dient als Mechanismus für das Stornieren eines clientseitigen Zertifikats. Wie bereits aus dem Namen hervorgeht, handelt es sich bei einer Zertifikatsperrliste um eine von einer Zertifizierungsstelle oder von einem delegierten CRL-Aussteller veröffentlichte Liste gesperrter Zertifikate. Das IVE unterstützt *Basis-CRLs*, die alle gesperrten Zertifikate des Unternehmens in einer vereinheitlichten Liste enthalten.

Das IVE erkennt die zu verwendende Zertifikatsperrliste anhand der Überprüfung des Clientzertifikats. (Beim Ausstellen eines Zertifikats schließt die Zertifizierungsstelle CRL-Informationen für das Zertifikat im Zertifikat selbst ein.) Damit sichergestellt ist, dass das IVE die aktuellsten CRL-Informationen erhält, kommuniziert es regelmäßig mit einem Sperrlisten-Verteilungspunkt, um eine aktualisierte Liste der gesperrten Zertifikate abzurufen. Bei einem *Sperrlisten-Verteilungspunkt (CRL distribution point, CDP)* handelt es sich um einen Speicherort auf einem LDAP-Verzeichnisserver oder auf einem Webserver, der von einer Zertifizierungsstelle zum Veröffentlichen von Zertifikatsperrlisten verwendet wird. Das IVE lädt die Zertifikatsperrlisteninformationen vom Sperrlisten-Verteilungspunkt herunter. Dieser Download erfolgt in dem in der Sperrliste angegebenen Intervall, in dem von Ihnen während der CRL-Konfiguration angegebenen Intervall und beim manuellen Herunterladen der Zertifikatsperrliste. Das IVE unterstützt auch die Aufteilung von Zertifikatssperrlisten. Die Aufteilung von Zertifikatssperrlisten ermöglicht Ihnen die Überprüfung von Teilen sehr großer Sperrlisten. Auf diese Weise müssen Sie nicht die Zeit und erforderliche Bandbreite aufbringen, um auf eine sehr große Sperrliste oder eine Sammlung großer Listen zuzugreifen und diese zu überprüfen. Die CRL-Aufteilung ist nur auf dem IVE aktiviert, wenn Sie die unten beschriebene Methode **Festlegen der CDP(s) im Client-Zertifikat** verwenden. In diesem Fall validiert das IVE den Benutzer, indem es *nur* die im Clientzertifikat angegebene Zertifikatssperrliste überprüft.

Zertifizierungsstellen schließen zwar CRL-Informationen in clientseitigen Zertifikaten ein, die Daten für Sperrlisten-Verteilungspunkte werden jedoch nicht immer berücksichtigt. Eine Zertifizierungsstelle hat folgende Möglichkeiten, um das IVE über den Ort des Sperrlisten-Verteilungspunkts eines Zertifikats zu informieren:

- **Festlegen der CDP(s) im CA-Zertifikat** – Wenn die Zertifizierungsstelle CA-Zertifikate ausstellt, kann sie dabei ein Attribut hinzufügen, das den Ort der/des Sperrlisten-Verteilungspunkte(s) angibt, auf den das IVE zugreifen soll. Wenn mehrere Sperrlisten-Verteilungspunkte angegeben sind, wählt das IVE den ersten im Zertifikat aufgelisteten Punkt und wechselt dann ggf. zu den nachfolgenden Sperrlisten-Verteilungspunkten.

- **Festlegen der CDP(s) im Client-Zertifikat** – Wenn die Zertifizierungsstelle Client-Zertifikate ausstellt, kann sie dabei ein Attribut hinzufügen, das den Ort der/des Sperrlisten-Verteilungspunkte(s) angibt, auf den das IVE zugreifen soll. Wenn mehrere Sperrlisten-Verteilungspunkte angegeben sind, wählt das IVE den ersten im Zertifikat aufgelisteten Punkt und wechselt dann ggf. zu den nachfolgenden Sperrlisten-Verteilungspunkten. Wenn das IVE die CRL-Aufteilung verwendet und im Clientzertifikat nur eine Zertifikatssperrliste angegeben ist, führt das IVE die Überprüfung *nur* anhand dieser Zertifikatssperrliste aus.

HINWEIS: Wenn Sie sich diese Methode auswählen, erhält der Benutzer bei der ersten Anmeldung beim IVE eine Fehlermeldung, weil keine CRL-Informationen verfügbar sind. Nachdem das IVE das Clientzertifikat erkannt und den CRL-Ort extrahiert hat, kann es mit dem Herunterladen der Zertifikatsperrliste beginnen und anschließend das Zertifikat des Benutzers überprüfen. Zwecks erfolgreicher Anmeldung beim IVE muss der Benutzer nach ein paar Sekunden erneut versuchen, die Verbindung herzustellen.

- **Auffordern des Administrators zur manuellen Eingabe des Orts des Sperrlisten-Verteilungspunktes** – Wenn die Zertifizierungsstelle keinen Ort des Sperrlisten-Verteilungspunktes in den Client- oder Zertifizierungsstellenzertifikaten angegeben hat, müssen Sie beim Konfigurieren des IVE manuell festlegen, wie das gesamte CRL-Objekt heruntergeladen werden soll. Sie können einen primären und einen Sicherungs-Sperrlisten-Verteilungspunkt angeben. (Die manuelle Eingabe des Orts des Sperrlisten-Verteilungspunktes bietet Ihnen die größte Flexibilität, da Sie die Zertifikate nicht neu ausstellen müssen, wenn Sie den Ort des Sperrlisten-Verteilungspunktes ändern.)

Das IVE überprüft das Zertifikat des Benutzers während der Authentifizierung anhand der entsprechenden Zertifikatsperrliste. Wenn das IVE ermittelt, dass das Zertifikat des Benutzers gültig ist, werden die Zertifikatattribute zwischengespeichert und ggf. bei den Überprüfungen der Rollen und Ressourcenrichtlinien angewendet. Wenn das IVE ermittelt, dass das Zertifikat des Benutzers ungültig ist, wenn es nicht die entsprechende Zertifikatsperrliste abrufen kann oder die Zertifikatsperrliste abgelaufen ist, wird dem Benutzer der Zugriff verweigert.

Konfigurieren Sie die CRL-Prüfung auf der Seite **System > Configuration > Certificates > Trusted Client CAs** in der Webkonsole.

HINWEIS:

- Das IVE unterstützt nur Zertifikatsperrlisten im PEM- oder DER-Format, die von der Zertifizierungsstelle, für die diese Sperrungen gelten, signiert wurden.
- Das IVE speichert nur die erste Zertifikatsperrliste in einer PEM-Datei.
- Das IVE bietet keine Unterstützung für die IDP-Erweiterung (Issuing Distribution Point) für Zertifikatsperrlisten.

Konfigurationsanweisungen finden Sie unter „Festlegen von CDP-Optionen“ auf Seite 177.

OCSP

Das OCSP-Protokoll (Online Certification Status Protocol) bietet Ihnen die Möglichkeit, Clientzertifikate in Echtzeit zu überprüfen. Bei Verwendung von OCSP wird das IVE zum Client eines OCSP-Responders und leitet Überprüfungsanfragen für Benutzer basierend auf Clientzertifikaten weiter. Der OCSP-Responder verwaltet einen Speicher von Zertifikatssperrlisten, die von CAs veröffentlicht wurden, und eine aktuelle Liste von gültigen und ungültigen Clientzertifikaten. Sobald der OCSP-Responder eine Überprüfungsanfrage vom IVE empfängt (im Allgemeinen eine HTTP- oder HTTPS-Übertragung), überprüft er den Status des Zertifikats entweder anhand seiner eigenen Authentifizierungsdatenbank, oder er wendet sich an den OCSP-Responder, der das Zertifikat ursprünglich ausgestellt hat, damit dieser die Anfrage überprüft. Nach dem Formulieren einer Antwort sendet der OCSP-Responder die signierte Antwort an das IVE, und das Originalzertifikat wird abhängig von der Bestätigung durch den OCSP-Responder genehmigt oder abgelehnt. Anweisungen zum Aktivieren und Konfigurieren von OCSP-Optionen finden Sie unter „Registerkarte „Trusted Client CAs““ auf Seite 170.

CAs vertrauter Server

Wenn Sie eine Webbrowsing-Lizenz besitzen, können Sie die Anmeldeinformationen für Websites validieren, auf die die Benutzer über die IVE-Appliance zugreifen. Sie müssen hierzu nur das Zertifizierungsstellenzertifikat der vertrauten Webserver für die IVE-Appliance installieren. (Alle vertrauten Stammzertifizierungsstellen für Webzertifikate sind in Internet Explorer 6.0 und Windows XP Service Pack 2 installiert. Diese Komponenten sind in der IVE-Appliance vorinstalliert.) Besucht ein Benutzer eine SSL-fähige Website, wird von der IVE-Appliance Folgendes überprüft:

- Das Zertifikat der Website wurde von einer der auf der IVE-Appliance installierten vertrauten Stammzertifizierungsstellen ausgestellt.
- Das Zertifikat der Website ist nicht abgelaufen.
- Der Wert Subject CN des Websitezertifikats stimmt mit dem Hostnamen des URL überein, auf den zugegriffen wurde. (Die IVE-Appliance lässt im Wert von Subject CN Platzhalter im folgenden Format zu: *.firma.com.)

Wird eine dieser Bedingungen nicht erfüllt, trägt die IVE-Appliance ein Hauptereignis ins Benutzerzugriffsprotokoll ein. Anschließend wird dem Benutzer der Zugriff auf die Website abhängig von den Einstellungen auf Rollenebene, die auf der Registerkarte **Users > Roles >** *Rollenname* **> Web > Options** der Webkonsole konfiguriert wurden, entweder gewährt oder verweigert. (Konfigurieren Sie diese Einstellungen nicht, warnt die IVE-Appliance den Benutzer zwar, dass das Websitezertifikat ungültig ist, lässt ihn aber dennoch auf die Website zugreifen.)

Auf der Seite **System > Configuration > Certificates > Trusted Server CAs** der Webkonsole können Sie das Zertifizierungsstellenzertifikat der vertrauten Webserver installieren. Anweisungen hierfür finden Sie unter „Hochladen von Zertifikaten der vertrauten Serverzertifizierungsstelle in das IVE“ auf Seite 180.

Codesignaturzertifikate

Wenn das IVE ein signiertes Java-Applet vermittelt, signiert es das Applet mit einem selbst signierten Zertifikat neu, das von einer nicht standardmäßig vertrauenswürdigen Stammzertifizierungsstelle ausgestellt wurde. Wenn ein Benutzer ein Applet anfordert, das Aufgaben mit einem hohen Risikopotential durchführt, z. B. Zugreifen auf Netzwerkserver, wird im Browser des Benutzers in einer Sicherheitswarnung angezeigt, dass der Stamm nicht vertrauenswürdig ist. Um die Anzeige dieser Warnung zu vermeiden, können Sie ein Codesignaturzertifikat importieren, mit dem das IVE zu vermittelnde Applets neu signiert.

Das IVE unterstützt die folgenden Arten von Codesignaturzertifikaten:

- **Microsoft Authenticode-Zertifikat** – Mit diesem Zertifikat signiert das IVE Applets, die über MS JVM oder SUN JVM ausgeführt werden. Beachten Sie, dass nur von Verisign ausgestellte Microsoft Authenticode-Zertifikate unterstützt werden. Microsoft Authenticode-Zertifikate sind unter folgender Adresse erhältlich:

  http://www.verisign.com/products-services/security-services/code-signing/index.html

- **JavaSoft-Zertifikat** – Mit diesem Zertifikat signiert das IVE Applets, die über SUN JVM ausgeführt werden. Beachten Sie, dass nur von Verisign und Thawte ausgestellte JavaSoft-Zertifikate unterstützt werden.

Beachten Sie bei der Auswahl des zu importierenden Codesignaturzertifikats folgende Browserabhängigkeiten:

- **Internet Explorer** – Auf neuen Computern, auf denen bei der Lieferung Windows XP vorinstalliert ist, wird in Internet Explorer normalerweise die SUN JVM ausgeführt. Dies bedeutet, dass Applets vom IVE mit dem JavaSoft-Zertifikat neu signiert werden müssen.

  Auf PCs unter Windows 98 oder 2000 oder auf PCs, die auf Windows XP aktualisiert wurden, wird in Internet Explorer normalerweise MS JVM ausgeführt. Dies bedeutet, dass Applets vom IVE mit einem Authenticode-Zertifikat neu signiert werden müssen.

- **Netscape, Firefox, und Safari** – Diese Browser unterstützen nur die SUN JVM. Dies bedeutet, dass Applets vom IVE mit dem JavaSoft-Zertifikat neu signiert werden müssen.

Weitere Hinweise für Benutzer der SUN JVM:

- Standardmäßig werden Applets vom Java-Plug-In zusammen mit dem Codesignaturzertifikat zwischengespeichert, das beim Benutzerzugriff auf das Applet bereitgestellt wird. Das bedeutet, dass der Browser Applets auch nach dem Importieren eines Codesignaturzertifikats in das IVE weiterhin mit dem ursprünglichen Zertifikat bereitstellt. Um sicherzustellen, dass Benutzer der SUN JVM keine Aufforderungen für nicht vertrauenswürdige Zertifikate für Applets erhalten, auf die sie vor dem Import eines Codesignaturzertifikats zugegriffen haben, muss der Cache des Java-Plug-Ins geleert werden. Alternativ können Benutzer den Cache deaktivieren. Durch diese Option kann jedoch die Leistung beeinträchtigt werden, da das Applet bei jedem Benutzerzugriff abgerufen werden muss.

- Das Java-Plug-In verwaltet eine eigene Liste vertrauenswürdiger Webserverzertifikate, die sich von der entsprechenden Liste des Browsers unterscheidet. Wenn ein Benutzer auf ein Applet zugreift, stellt die SUN JVM (zusätzlich zum Browser) eine eigene Verbindung mit dem Webserver her, auf dem sich das Applet befindet. Dem Benutzer wird daraufhin die Option zur Verfügung gestellt, zusätzlich zum Codesignaturzertifikat das Webserverzertifikat anzunehmen. In solchen Fällen muss der Benutzer die Schaltfläche Always Trust für das Webserverzertifikat auswählen. Aufgrund einer integrierten Zeitüberschreitung im Java-Plug-In wird das Applet nicht geladen, wenn der Benutzer bei der Auswahl dieser Schaltfläche für das Webserverzertifikat zu lange wartet.

Aufgabenzusammenfassung: Konfiguration des IVE zum Signieren oder Neusignieren von Java-Applets

Zur Konfiguration des IVE zum Neusignieren von Applets mittels Codesignaturzertifikaten sind folgende Schritte notwendig:

1. Installation der Serverzwischenzertifikate über die Seite **System > Configuration > Certificates > Code-Signing Certificates** in der Webkonsole. Anweisungen hierfür finden Sie unter „Importieren eines Codesignaturzertifikats“ auf Seite 181.

2. Führen Sie einen der folgenden Vorgänge aus:

   - Erstellen von Codesignaturrichtlinien, die festlegen, welche Applets vom IVE auf der Seite **Resource Policies > Web > Java > Code Signing** in der Webkonsole neu signiert werden. Die Richtlinien müssen die Namen der Hosts angeben, von denen die Applets stammen. Anweisungen hierfür finden Sie unter „Schreiben einer Ressourcenrichtlinie für die Java-Codesignatur“ auf Seite 318.

   - Laden Sie Ihre eigenen Java-Applets auf das IVE hoch, und lassen Sie sie vom IVE signieren oder neu signieren, wie unter „Aufgabenzusammenfassung: Hochladen und Aktivieren von Java-Applets“ auf Seite 115 beschrieben.

Endpoint Defense – Übersicht

Juniper Networks hat die Juniper Endpoint Defense Initiative (J.E.D.I.) als umfangreiche Lösung für die Einschätzung der Vertrauenswürdigkeit von Secure Access 700 Endpunkten entwickelt. Bei der J.E.D.I. kommt eine mehrschichtige Herangehensweise zur Anwendung, die die endpunktbezogenen Risiken für Unternehmensnetzwerke minimieren soll. Durch die Verwendung von J.E.D.I.-Komponenten können Sie die Systeme von Benutzern außerhalb und innerhalb Ihres Netzwerkes sichern, bevor Sie diesen erlauben, eine Verbindung zu Ihrem IVE herzustellen. Zu den J.E.D.I.-Komponenten gehören:

- **Host Checker** – Bei Host Checker (auch systemeigene Hostprüfung und richtlinienbasierte Durchführung genannt) handelt es sich um eine systemeigene IVE-Komponente, mit der Sie Endpunktüberprüfungen auf Hosts durchführen können, die mit dem IVE eine Verbindung herstellen. Auf Hosts, die unter Windows, Macintosh oder Linux betrieben werden, können Sie mit Hilfe von Host Checker sicherstellen, dass bestimmte Prozesse, Dateien oder Ports mit den von Ihnen gemachten Angaben übereinstimmen, bevor Sie einem Benutzer den Zugriff auf einen IVE-Bereich oder eine IVE-Rolle gewähren. Auf Hosts, die unter Windows betrieben werden, kann Host Checker auch zur Überprüfung von Registrierungseinträgen und zum Arbeiten mit integrierten Drittanbieterprodukten für die Endpunktsicherheit verwendet werden. So können Sie die Funktionalität von Host Checker zum Prüfen von Drittanbieterprodukten nutzen, um festzulegen, dass ein Benutzer nur dann auf eine bestimmte IVE-Rolle zugreifen kann, wenn eine Antivirenanwendung auf seinem Computer aktiviert ist. Wenn der Computer des Benutzers keine der Host Checker-Anforderungen erfüllt, kann eine Hilfsoptionsseite angezeigt werden, die Anweisungen und Links zu Ressourcen enthält, mit deren Hilfe der Benutzer den Computer mit den Sicherheitsanforderungen in Einklang bringen kann. Weitere Informationen finden Sie unter „Host Checker – Übersicht“ auf Seite 75.

- **Host Check Client Interface (nur Windows)** – Bei der Clientschnittstelle für die Hostprüfung handelt es sich um eine API, über die Sie mithilfe von Host Checker Ihre eigenen DLLs ausführen können. Über die Schnittstelle können Sie veranlassen, dass Host Checker eine DLL ausführt, die bereits auf dem System des Benutzers installiert oder als Teil eines proprietären Betriebssystemimage verteilt wurde. Das schließt Programme mit ein, die die Kompatibilität mit proprietären Images, Antivirensoftware und Clients mit persönlicher Firewall prüfen. Host Checker führt die jeweilige DLL bei der Anmeldung des Benutzers beim IVE aus. Alle nachfolgenden Aktionen richten sich nach der Rückmeldung von der DLL. So können Sie beispielsweise einem Benutzer den Zugriff auf das IVE verweigern, wenn bei der Überprüfung der Clientsoftware ein Fehler auftritt. Weitere Informationen finden Sie im Handbuch *J.E.D.I. Solution Guide*, verfügbar auf der Juniper-Supportsite.

- **Host Check Server Integration Interface (nur Windows)** – Bei der Server-Integrationsschnittstelle für die Hostprüfung handelt es sich um eine API, mit der Sie ein J.E.D.I.-kompatibles System eng in das IVE integrieren können. Wie mit der Clientschnittstelle können Sie auch mit Hilfe der Server-Integrationsschnittstelle für die Hostprüfung festlegen, dass im Zuge der Hostprüfung Softwareprogramme eines Drittanbieters auf dem Client ausgeführt werden. Hierzu gehören Hostintegritätsprüfungen, Programme zur

Malwareerkennung und virtuelle Umgebungen. Darüber hinaus können Sie über diese Schnittstelle für unterschiedliche Ergebnisse der diversen Richtlinienüberprüfungen von Drittanbieteranwendungen sehr detailliert festlegen, welche Schritte von Host Checker im Einzelnen ausgeführt werden sollen. So können Sie Benutzer basierend auf den Ergebnissen einzelner Richtlinien dynamisch bestimmten Bereichen, Rollen und Ressourcen zuordnen. Weitere Informationen finden Sie im Handbuch *J.E.D.I. Solution Guide*, verfügbar auf der Juniper-Supportsite.

- **Cache Cleaner (nur Windows)** – Bei Cache Cleaner handelt es sich um eine systemeigene IVE-Komponente, mit der übrig gebliebene Daten wie z. B. Cookies, temporäre Dateien oder Inhalte des Anwendungscache nach einer IVE-Sitzung vom Benutzercomputer entfernt werden können. Cache Cleaner trägt zur Sicherung des Benutzersystems bei, indem die Anwendung verhindert, dass nachfolgende Benutzer temporäre Kopien von Dateien suchen können, die sich der vorhergehende Benutzer angesehen hat, und indem Webbrowser daran gehindert werden, die von Benutzern in Webformularen eingegebenen Benutzernamen, Kennwörter und Webadressen dauerhaft zu speichern. Weitere Informationen finden Sie unter „Cache Cleaner – Übersicht“ auf Seite 87.

Die Verwendung dieser Endpoint Defense-Komponenten ermöglicht einen mehrstufigen Sicherungsansatz, mit dem Sie eine Vielzahl von Endpunktprüfungen im IVE verwalten und bereitstellen können. So können Sie z. B. eine Prüfung auf Antivirensoftware oder Software für eine persönliche Firewall durchführen, bevor Sie einem Benutzer Zugriff auf einen der IVE-Bereiche gewähren. Darüber hinaus können Sie ggf. die Software auf dem System des Benutzers starten, dem Benutzer auf der Grundlage einzelner Richtlinien in Ihrer DLL Rollen zuordnen und den Zugriff auf einzelne Ressourcen je nach Vorhandensein einer Spyware-Erkennungssoftware weiter einschränken.

Anschließend können Sie mit Cache Cleaner übrig gebliebene Dateien entfernen und den Anwendungscache des Benutzers leeren, wenn dieser seine IVE-Sitzung beendet hat.

Host Checker – Übersicht

Host Checker ist ein clientseitiger Agent, der Endpunktsicherheitsprüfungen auf Hosts durchführt, die mit dem IVE eine Verbindung herstellen. So kann Host Checker bei der Auswertung einer Rollenzuordnungsregel oder Ressourcenrichtlinie aufgerufen werden, bevor dem jeweiligen Benutzer eine IVE-Anmeldeseite angezeigt wird. Das IVE kann die Endpunkteigenschaften auf Hosts mit Hilfe der folgenden Verfahren überprüfen:

- **Host Checker-Implementierung einer unterstützten Anwendung für die Endpunktsicherheit (nur Windows)** – Der clientseitige Agent von Host Checker ruft die Host Checker-Integrationsfunktion des angegebenen Endpunktsicherheitsprodukts eines Drittanbieters auf und ermittelt anhand des Rückgabewerts, ob das Produkt entsprechend den konfigurierten Richtlinien ausgeführt wird (siehe „Richtlinien für Host Checker definieren“ auf Seite 76).

- **Integration von Host Checker anhand einer benutzerdefinierten DLL (nur Windows)** – Die Clientschnittstelle für die Hostprüfung ermöglicht Ihnen das Integrieren einer DLL, die benutzerdefinierte clientseitige Überprüfungen ausführt. Sie müssen diese DLL auf jedem Clientcomputer installieren.

- **Attributüberprüfung** – Unter Windows, Macintosh oder Linux sucht Host Checker nach den Spuren der angegebenen Anwendung, einschließlich Prozessen oder Dateien. Unter Windows prüft Host Checker auch Registrierungseinträge.

Wenn der Computer des Benutzers keine der Host Checker-Anforderungen erfüllt, kann dem Benutzer eine Hilfsoptionsseite angezeigt werden. Diese speziell zugeschnittene HTML-Seite kann Ihre Anweisungen sowie Links zu Ressourcen enthalten, mit deren Hilfe der Benutzer den Computer mit den Sicherheitsanforderungen jeder Host Checker-Richtlinie in Einklang bringen kann.

Weitere Informationen finden Sie unter:

- „Richtlinien für Host Checker definieren“ auf Seite 76
- „Implementieren von Host Checker-Richtlinien“ auf Seite 81
- „Host Checker-Hilfsoption verwenden“ auf Seite 78
- „Richtlinienserver für Host Checker-Clients verfügbar machen“ auf Seite 82
- „Installieren von Host Checker“ auf Seite 83
- „Ausführen von Host Checker-Richtlinien“ auf Seite 84
- „Aufgabenzusammenfassung: Konfigurieren von Host Checker“ auf Seite 86

Richtlinien für Host Checker definieren

Um Host Checker zum Durchsetzen von Richtlinien für die Verwaltung von Endpunkten verwenden zu können, müssen Sie globale Richtlinien für Host Checker erstellen und diese anschließend auf Bereichs- und Rollenebene implementieren.

Beim Erstellen von Host Checker-Richtlinien über die Webkonsole können Sie Hostprüfungsmethoden und/oder Regeleinstellungen festlegen. Bei einer *Hostprüfungsmethode* handelt es sich um die Implementierung des Endpunktsicherheitsprodukts eines Drittanbieters für Host Checker. Durch die Methode wird festgestellt, ob eine Anwendung in Übereinstimmung mit den konfigurierten Richtlinien ausgeführt wird. Auf Windows-Clients bietet Host Checker Methoden für:

- Sygate Enforcement API
- Sygate Security Agent
- Zone Labs: ZoneAlarm Pro und Zone Labs Integrity
- McAfee Desktop Firewall 8.0
- InfoExpress CyberGatekeeper Agent

Bei einer *Hostprüfungsregel* handelt es sich um eine Anforderung, die von einem Client erfüllt werden muss, damit Host Checker eine Erfolgsmeldung an das IVE zurückgibt. Sie können fünf Typen von Regeln festlegen:

- **3rd Party NHC check (nur Windows)** – Geben Sie mit dieser Regel den Speicherort einer benutzerdefinierten DLL an, die mit der Clientschnittstelle für die Hostprüfung geschrieben wird. Host Checker ruft die DLL auf, um benutzerdefinierte clientseitige Überprüfungen auszuführen. Wenn die DLL eine Bestätigung an Host Checker zurückgibt, betrachtet das IVE die Regel als erfüllt. Weitere Informationen zum Erstellen einer benutzerdefinierten DLL mit Hilfe der Clientschnittstelle für die Hostprüfung finden Sie im Handbuch *J.E.D.I. Solution Guide*, verfügbar auf der Juniper-Supportsite.

- **Port check** – Bei einer Portprüfung werden die Netzwerkverbindungen überprüft, die ein Client während einer Sitzung herstellen kann. Verwenden Sie diese Regel, um von einem Clientcomputer das Öffnen bzw. Schließen bestimmter Ports für den Benutzerzugriff auf das IVE zu fordern.

- **Process check** – Bei einer Prozessprüfung wird die Software überprüft, die ein Client während einer Sitzung ausführt. Verwenden Sie diese Regel, um vom Clientcomputer das Ausführen bzw. Unterdrücken eines bestimmten Prozesses für den Benutzerzugriff auf das IVE zu fordern.

- **File check** – Verwenden Sie diese Regel, um von einem Clientcomputer das Vorhandensein bzw. das Fehlen einer bestimmten Datei für den Benutzerzugriff auf das IVE zu fordern. Dateiprüfungen können auch verwendet werden, um das Alter und den Inhalt von erforderlichen Dateien auszuwerten (mit Hilfe von MD5-Prüfsummen) und den Zugriff entsprechend zu gewähren bzw. zu verweigern.

- **Registry settings check (nur Windows)** – Bei einer Registrierungseinstellungsprüfung werden proprietäre PC-Images, Systemkonfigurationen und Softwareeinstellungen überprüft, die für den Clientzugriff auf das IVE erforderlich sind. Verwenden Sie diese Regel, um von einem Clientcomputer das Vorhandensein bestimmter Registrierungseinstellungen für den Benutzerzugriff auf das IVE zu fordern. Registrierungseinstellungsprüfungen können auch verwendet werden, um das Alter erforderlicher Dateien auszuwerten und den Zugriff entsprechend zu gewähren oder zu verweigern.

Für die Anzahl der Methoden und Regeln innerhalb einer Host Checker-Richtlinie bestehen keine Einschränkungen.

Sie können eine Richtlinie erstellen, die feststellt, ob alternative Attributsätze vorhanden sind. So können Sie die Operatoren AND und OR im folgenden Ausdruck benutzen, um zu prüfen, ob eine persönliche Firewall auf dem Client aktiviert ist, und ob wenigstens eine von zwei möglichen Antivirenanwendungen aktiv ist:

```
ZoneLabsFirewall AND (McAfeeAntivirus OR NortonAntivirus)
```

Sie können eine Richtlinie erstellen, die für Windows, Macintosh und Linux verschiedene Host Checker-Anforderungen erzwingt. Sie können z. B. eine Richtlinie erstellen, die auf jedem Betriebssystem unterschiedliche Dateien oder Prozesse überprüft.

Sie können Host Checker so konfigurieren, dass eine Verbindungssteuerungsrichtlinie erstellt wird, die Angriffe von anderen infizierten Computern aus demselben physischen Netzwerk auf Windows-Clientcomputer verhindert. Die Verbindungssteuerungsrichtlinie blockiert alle eingehenden TCP-Verbindungen und alle ein- und ausgehenden UDP-Pakete. Diese Richtlinie lässt den gesamten ausgehenden TCP- und Network Connect-Verkehr sowie alle Verbindungen mit DNS-Servern, WINS-Servern, DHCP-Servern, Proxyservern und dem IVE zu.

Verwenden Sie zum Erstellen globaler Host Checker-Richtlinien die Einstellungen auf der Seite **Signing In > End Point > Host Checker** der Webkonsole. Konfigurationsanweisungen finden Sie unter „Erstellen einer globalen clientseitigen Host Checker-Richtlinie“ auf Seite 208.

Durch die Aktivierung der dynamischen Richtlinienauswertung von Host Checker werden die Rollen einzelner Benutzer automatisch aktualisiert. Host Checker kann das IVE veranlassen, bei jeder Änderung des Host Checker-Status eines Benutzers Ressourcenrichtlinien auszuwerten. (Wenn die dynamische Richtlinienauswertung für Host Checker nicht aktiviert ist, wertet das IVE zwar keine Ressourcenrichtlinien aus, die Authentifizierungsrichtlinie, Rollenzuordnungsregeln und Rolleneinschränkungen werden dennoch bei jeder Änderung des Host Checker-Status eines Benutzers ausgewertet.) Weitere Informationen finden Sie unter „Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)“ auf Seite 44.

Auf Windows-Clients können Sie Host Checker-Richtlinien auch über die Server-Integrationsschnittstelle für die Hostprüfung definieren. Beim Hochladen des Drittanbieter-Integrationspakets auf das IVE werden diese Richtlinientypen automatisch vom IVE erkannt. Weitere Informationen finden Sie im Handbuch *J.E.D.I. Solution Guide*, verfügbar auf der Juniper-Supportsite.

Host Checker-Hilfsoption verwenden

Bei der Definition einer Richtlinie für Host Checker können Sie auch Hilfsoptionen festlegen, die Host Checker anbieten soll, wenn ein Benutzercomputer die Anforderungen der Richtlinie nicht erfüllt. So können Sie das IVE so konfigurieren, dass dem Benutzer eine Hilfsoptionsseite angezeigt wird. Diese Seite kann Ihre Anweisungen sowie Links zu Ressourcen enthalten, mit deren Hilfe der Benutzer den Computer mit den Host Checker-Richtlinienanforderungen in Einklang bringen kann.

So kann dem Benutzer eine Hilfsoptionsseite angezeigt werden, die z. B. die folgenden Anweisungen und den folgenden Link enthält:

Die Sicherheit des Computers ist nicht ausreichend.

Ihr Computer entspricht nicht den folgenden Sicherheitsanforderungen. Gehen Sie zum Korrigieren der Probleme wie unten beschrieben vor. Klicken Sie abschließend auf **Try Again**. Wenn Sie ohne Korrektur der Probleme **Continue** wählen, haben Sie möglicherweise keinen Zugriff auf alle Intranetserver.

1. TrendMicro

Anweisungen: Sie verfügen nicht über die aktuellsten Signaturdateien. **Klicken Sie hier, um die aktuellsten Signaturdateien herunterzuladen.**

2. ManagedPC

Anweisungen: Melden Sie sich über den Virtual Desktop erneut beim IVE an.

Sie können für jede Host Checker-Richtlinie zwei Arten von Hilfsoptionen konfigurieren:

- **User-driven** – Mithilfe benutzerdefinierter Anweisungen kann der Benutzer über die fehlgeschlagene Richtlinie und darüber, wie er den Computer mit der Richtlinie in Einklang bringen kann, informiert werden. Die nötigen Schritte für eine erfolgreiche Neuauswertung der fehlgeschlagenen Richtlinie müssen vom Benutzer vorgenommen werden.

- **Automatic (system-driven)** – Host Checker kann so konfiguriert werden, dass die Hilfsoptionen für den Benutzercomputer automatisch ausgeführt werden. So können Prozesse beendet, Dateien gelöscht oder andere Richtlinien gestartet werden. Unter Windows kann auch die API-Funktion Remediate () als Teil einer J.E.D.I.-DLL aufgerufen werden. Host Checker informiert Benutzer nicht über automatisch vorgenommene Aktionen. (Sie können natürlich Informationen über automatische Aktionen in Ihre benutzerdefinierten Anweisungen mit aufnehmen.)

Für jede Richtlinie können einzelne oder alle der folgenden Hilfsoptionen für Windows-, Macintosh- oder Linux-Clientcomputer aktiviert werden:

- **Enable Custom Instructions (user-driven)** – Über die Host Checker-Hilfsoptionsseite können Sie für den Benutzer Anweisungen zusammen mit Links zu Ressourcen wie Richtlinienservern oder Websites anzeigen.

- **Evaluate other policies (automatic)** – Sie können eine oder mehrere Richtlinien definieren, die von Host Checker ausgewertet werden sollen, falls die aktuellen Richtlinienanforderungen nicht erfüllt werden. Wenn ein Benutzer beispielsweise versucht, von einem Clientcomputer außerhalb des Netzwerks (z. B. von einem Kiosk aus) auf das IVE zuzugreifen, können Sie diese Option aktivieren, um eine alternative Richtlinie auszuwerten, die den Zugriff des Benutzers auf das IVE über eine Sygate Virtual Desktop-Umgebung fordert.

- **Kill Process (automatic)** – Sie können Prozesse beenden, wenn der Clientcomputer die aktuellen Richtlinienanforderungen nicht erfüllt.

- **Delete Files (automatic)** – Sie können Dateien löschen, wenn der Clientcomputer die aktuellen Richtlinienanforderungen nicht erfüllt.

Diese Hilfsoptionen können sowohl in Client- als auch in Serverrichtlinien aktiviert werden. Konfigurationsanweisungen finden Sie unter „Erstellen einer globalen clientseitigen Host Checker-Richtlinie“ auf Seite 208 oder „Erstellen einer globalen Serverrichtlinie“ auf Seite 215.

Host Checker-Hilfsoptionen für den Benutzer

Die Hilfsoptionsseite wird in folgenden Situationen angezeigt:

- **Vor der Anmeldung**:
  - Haben Sie benutzerdefinierte Anweisungen für fehlgeschlagene Richtlinien aktiviert, zeigt das IVE dem Benutzer die Hilfsoptionsseite an. Der Benutzer hat zwei Möglichkeiten:
    - Er ergreift die geeigneten Maßnahmen, um den Computer mit der Richtlinie in Einklang zu bringen, und klickt anschließend auf der Hilfsoptionsseite auf die Schaltfläche **Try Again**. Host Checker prüft erneut, ob der Computer des Benutzers die Richtlinie erfüllt.
    - Er nimmt keine Änderungen vor und klickt auf die Schaltfläche **Continue**, um sich beim IVE anzumelden. Er kann nicht auf den Bereich, die Rolle oder die Ressource zugreifen, welche die Erfüllung der gescheiterten Richtlinie erfordert.

HINWEIS: Wenn Sie für das IVE nicht wenigstens einen Bereich konfigurieren, für den keine Erfüllung einer Host Checker-Richtlinie erzwungen wird, muss der Benutzer seinen Computer erst mit den erzwungenen Richtlinien in Einklang bringen, bevor er sich beim IVE anmeldet.

  - Wenn Sie keine benutzerdefinierten Anweisungen für fehlgeschlagene Richtlinien aktiviert haben, zeigt Host Checker dem Benutzer die Hilfsoptionsseite nicht an. Stattdessen zeigt das IVE die Anmeldeseite an, verweigert dem Benutzer aber den Zugriff auf sämtliche Bereiche, Rollen oder Ressourcen mit einer gescheiterten Host Checker-Richtlinie.

- **Nach dem Anmelden**:
  - **(nur Windows)** Wenn der Windows-Computer eines Benutzers während einer Sitzung nicht mehr den Richtlinienanforderungen von Host Checker entspricht, wird ein Symbol auf der Taskleiste angezeigt, und eine Popupmeldung wird eingeblendet, die den Benutzer von der Nichterfüllung in Kenntnis setzt. Der Benutzer kann auf die Popupmeldung klicken, um die Hilfsoptionsseite anzuzeigen.
  - **(Macintosh oder Linux)** Wenn der Macintosh- oder Linux-Computer eines Benutzers während einer Sitzung nicht mehr den Richtlinienanforderungen von Host Checker entspricht, zeigt das IVE die Hilfsoptionsseite an, um den Benutzer von der Nichterfüllung in Kenntnis zu setzten.

HINWEIS: Wenn der Benutzer die Hilfsoptionsseite mit Hilfe seiner persönlichen Einstellungen ausblendet, kann er nur dann über den sicheren Gateway fortfahren, wenn Sie andere Bereiche und Rollen konfigurieren, die keine Host Checker-Richtlinie erzwingen.

Implementieren von Host Checker-Richtlinien

Nachdem Sie globale Richtlinien über die Seite **Signing In > End Point > Host Checker** der Webkonsole erstellt haben, können Sie den IVE- und Ressourcenzugriff einschränken, indem die Ausführung von Host Checker in folgenden Komponenten gefordert wird:

- **Richtlinie für die Bereichsauthentifizierung** – Wenn Administratoren oder Benutzern versuchen, sich am IVE anzumelden, wertet das IVE die Authentifizierungsrichtlinie des angegebenen Bereichs aus, und es ermittelt, ob für die Authentifizierung auch Host Checker ausgeführt werden muss. In der Konfiguration einer Richtlinie für die Bereichsauthentifizierung können Sie festlegen, dass Host Checker entweder lediglich heruntergeladen wird, dass außerdem die für den Bereich festgelegte Host Checker-Richtlinien durchgesetzt werden oder dass Host Checker nicht erforderlich ist. Der Benutzer muss sich über einen Computer anmelden, der den für den Bereich festgelegten Host Checker-Anforderungen entspricht. Erfüllt der Computer des Benutzers die Anforderungen nicht, verweigert das IVE dem Benutzer den Zugriff, sofern Sie keine Hilfsoptionen konfiguriert haben, mit deren Hilfe der Benutzer seinen Computer mit den Sicherheitsanforderungen in Einklang bringen kann. Sie können Einschränkungen auf Bereichsebene über die Seite **Administrators/Users > Authentication >** *Ausgewählter Bereich* **> Authentication Policy > Host Checker** in der Webkonsole konfigurieren.

- **Rolle** – Wenn das IVE ermittelt, welche Rollen einem Administrator oder Benutzer zugeordnet werden können, wertet es die Einschränkungen der einzelnen Rollen aus. Dabei wird festgelegt, ob der Computer des Benutzers für die Rolle bestimmte Host Checker-Richtlinien erfüllen muss. Wenn dies der Fall ist und der Computer des Benutzers die festgelegten Host Checker-Richtlinien nicht erfüllt, erfolgt keine Rollenzuordnung durch das IVE, es sei denn, Sie konfigurieren Hilfsoptionen, mit Hilfe derer der Benutzer seinen Computer mit den Sicherheitsanforderungen in Einklang bringen kann. Sie können Einschränkungen auf Rollenebene über die Seite **Administrators > Delegation >** *Ausgewählte Rolle* **> General > Restrictions > Host Checker** in der Webkonsole oder über die Seite **Users > Role >** *Ausgewählte Rolle* **> General > Restrictions > Host Checker** konfigurieren.

Sie können festlegen, dass das IVE die Host Checker-Richtlinien nur beim erstmaligen Zugriffsversuch des Benutzers auf den Bereich, die Rolle oder die Ressource auswertet. Oder Sie legen fest, dass das IVE die Richtlinien während der Sitzung des Benutzers in regelmäßigen Abständen erneut auswerten soll. Bei einer periodischen Auswertung von Host Checker-Richtlinien ordnet das IVE die Benutzer dynamisch bestimmten Rollen zu und gewährt ihnen je nach den Ergebnissen der jeweils letzten Auswertung Zugriff auf neue Ressourcen. Weitere Informationen finden Sie unter „Ausführen von Host Checker-Richtlinien“ auf Seite 84.

Richtlinienserver für Host Checker-Clients verfügbar machen

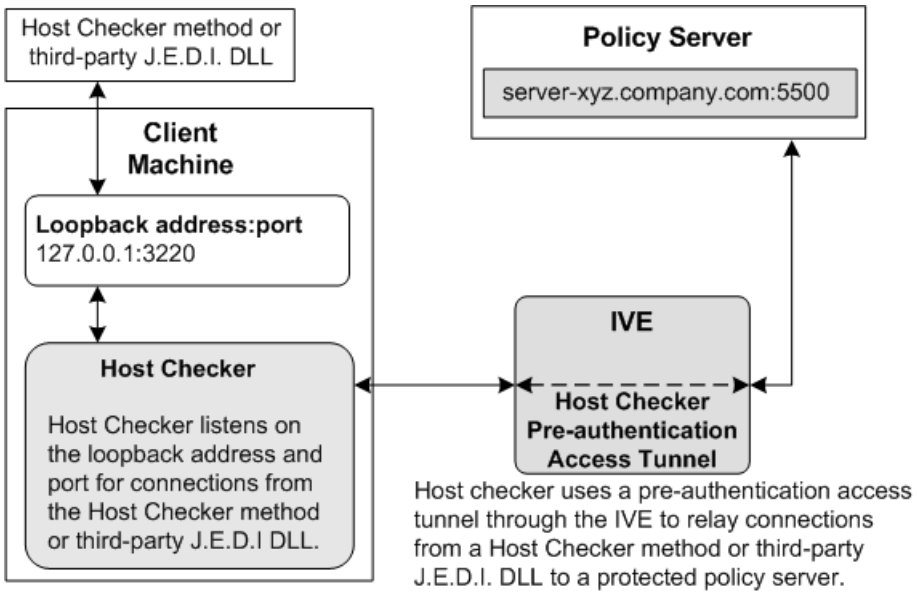
Wenn Ihre Richtlinien Host Checker-Methoden oder J.E.D.I.-DLLs von Drittanbietern für den Zugriff auf einen Richtlinienserver (oder eine andere Ressource) erfordern, um die Einhaltung der Sicherheitsanforderungen vor der Authentifizierung der Benutzer zu prüfen, können Sie mit Hilfe einer der folgenden Methoden die Ressource für die Windows-Clients von Host Checker verfügbar machen:

- **Stellen Sie den Richtlinienserver in einer DMZ bereit, in der Host Checker-Methoden oder J.E.D.I.-DLLs von Drittanbietern direkten Zugriff auf den Server haben und nicht über das IVE zugreifen müssen.** – Dies ist die einfachste Art der Bereitstellung, da Sie keinen Host Checker-Zugriffstunnel für die Authentifizierungs-Vorabprüfungen definieren müssen, der die Verbindung zwischen den Clients und dem Richtlinienserver über das IVE herstellt.

- **Stellen Sie den Richtlinienserver in einer geschützten Zone hinter dem IVE bereit (nur Windows)** – Für diese Art der Bereitstellung müssen Sie einen *Zugriffstunnel für die Authentifizierungs-Vorabprüfungen* definieren. Ein Zugriffstunnel für die Authentifizierungs-Vorabprüfungen ermöglicht Host Checker-Methoden oder J.E.D.I. DLLs von Drittanbietern den Zugriff auf den geschützten IVE-Richtlinienserver oder die Ressource, bevor Benutzer vom IVE authentifiziert werden. Zur Definition eines Zugriffstunnels für die Authentifizierungs-Vorabprüfungen ordnen Sie der IP-Adresse und dem Port des Richtlinienservers eine Loopbackadresse (oder einen Hostnamen) und einen Port des Clients zu. Fügen Sie eine oder mehrere Tunneldefinitionen einer Datei mit dem Namen MANIFEST.HCIF hinzu, und laden Sie diese anschließend auf das IVE hoch. Sie können mehrere MANIFEST.HCIF-Dateien auf das IVE hochladen. Für alle in einem Bereich aktiven Richtlinien von Drittanbietern erzeugt Host Checker Tunnels für alle Tunneldefinitionen der MANIFEST.HCIF Dateien, unter der Annahme, dass die Definitionen eindeutig sind. Konfigurationsanweisungen finden Sie unter „Hochladen eines Host Checker-Richtlinienpakets in das IVE“ auf Seite 219.

  Während des Betriebs auf einem Windows-Client prüft Host Checker alle von Ihnen in den Tunneldefinitionen festgelegten Loopbackadressen und Ports auf eine Verbindung. Verbindungen können durch die integrierten Host Checker-Methoden und durch Client- oder Server-J.E.D.I. DLLs zustande kommen. Host Checker verwendet Zugriffstunnel(s) für die Authentifizierungs-Vorabprüfungen zur Weiterleitung der Verbindungen über das IVE an die/den Richtlinienserver oder andere Ressourcen.

Abbildung 22: Host Checker erzeugt einen Tunnel von einem Client zu einem Richtlinienserver hinter dem IVE.


Host Checker method or third-party J.E.D.I. DLL
Client Machine
Loopback address:port
127.0.0.1:3220
Host Checker
Host Checker listens on the loopback address and port for connections from the Host Checker method or third-party J.E.D.I DLL.
Policy Server
server-xyz.company.com:5500
IVE
Host Checker Pre-authentication Access Tunnel
Host checker uses a pre-authentication access tunnel through the IVE to relay connections from a Host Checker method or third-party J.E.D.I. DLL to a protected policy server.

HINWEIS: Host Checker-Tunnel für den Zugriff vor der Authentifizierung werden nur unter Windows unterstützt.

Installieren von Host Checker

Wenn Sie eine Richtlinie auf einer Bereichs-, Rollen- oder Ressourcenrichtlinienebene implementieren, für die Host Checker erforderlich ist, müssen Sie einen Mechanismus bereitstellen, anhand dessen das IVE oder der Benutzer Host Checker auf dem Clientcomputer installieren kann. Andernfalls steht der Host Checker-Client beim Überprüfen der Host Checker-Richtlinie für eine Rückmeldung zum IVE nicht zur Verfügung, so dass dem Computer des Benutzers der Zugriff verweigert wird.

Für die Installation von Host Checker auf dem System eines Benutzers stehen zwei Methoden zu Auswahl:

- **Das IVE installiert Host Checker automatisch** – Aktivieren Sie die automatische Installation über die Seite **User/Administrator > Authentication > [Bereich] > Authentication Policy > Host Checker** in der Webkonsole. (Konfigurationsanweisungen finden Sie unter „Angeben von Host Checker-Einschränkungen“ auf Seite 423.) In diesem Fall wertet das IVE die Option auf Bereichsebene aus, sobald der Benutzer auf die IVE-Anmeldeseite zugreift, und überprüft, ob die aktuelle Version von Host Checker auf dem Computer des Benutzers installiert ist. Wenn Host Checker nicht installiert ist, versucht das IVE die Installation mit Hilfe der ActiveX- oder Java-Übertragungsmethode.

Wenn sich ein Windows-Benutzer am IVE anmeldet, versucht das IVE, ein ActiveX-Steuerelement auf dem Benutzersystem zu installieren. Wurde das ActiveX-Steuerelement erfolgreich installiert, verwaltet das Steuerelement die Installation von Host Checker.

Wenn das IVE das ActiveX-Steuerelement nicht installieren kann, da Administrator- oder Benutzerberechtigungen fehlen oder ActiveX auf dem Benutzersystem deaktiviert ist, versucht das IVE, Host Checker mit Java zu installieren. Auf Macintosh- und Linux-Hosts verwendet das IVE immer die Java-Übertragungsmethode. Die Java-Übertragungsmethode benötigt nur Benutzerberichtigungen; allerdings muss Java auf dem System des Benutzers aktiviert sein. Für den Firefox-Browser unter Linux müssen Java Runtime und Java-Plug-In installiert sein.

Kann das IVE die Java-Übertragungsmethode nicht verwenden, da Java deaktiviert ist, zeigt das IVE eine Fehlermeldung an.

- **Der Benutzer oder Administrator installiert Host Checker manuell (nur Windows)** – Laden Sie das Host Checker-Installationsprogramm von der Seite **Maintenance > System > Installers** in der Webkonsole herunter, und installieren Sie damit Host Checker auf dem System des Benutzers. (Konfigurationsanweisungen finden Sie unter „Registerkarte „Installers““ auf Seite 361.)

HINWEIS: Zum Installieren von Host Checker benötigen Benutzer wie unter „Installation von clientseitigen Anwendungen“ auf Seite 411 beschrieben entsprechende Berechtigungen. Wenn dies nicht gegeben ist, müssen Sie zum Umgehen dieser Anforderung den Juniper Installer Service verwenden, der Ihnen auf der Seite **Maintenance > System > Installers** in der Webkonsole zur Verfügung steht.

Ausführen von Host Checker-Richtlinien

Bei dem Versuch eines Benutzers, auf das IVE zuzugreifen, wertet Host Checker die Richtlinien in der folgenden Reihenfolge aus:

1. **Erstauswertung** – Beim erstmaligen Zugriffsversuch eines Benutzers auf die IVE-Anmeldeseite nimmt Host Checker eine erste Auswertung vor. Anhand der Methoden und Regeln, die Sie in den Richtlinien festgelegt haben, überprüft Host Checker, ob der Client die Endpunktsicherheitsanforderungen erfüllt und übermittelt das Ergebnis an das IVE. Die Erstauswertung erfolgt unabhängig davon, ob die Host Checker-Richtlinien auf Bereichs- oder Rollenebene implementiert wurden.

   Wenn der Benutzer die IVE-Anmeldeseite nach dem Starten von Host Checker und vor dem Anmelden am IVE verlässt, wird Host Checker auf dem Computer des Benutzers ausgeführt, bis der Vorgang durch eine Zeitbegrenzung abgebrochen wird.

   Erhält das IVE von Host Checker aus unbestimmten Gründen (einschließlich manueller Beendigung von Host Checker durch den Benutzer) keine Ergebnisse, zeigt das IVE eine Fehlermeldung an, und fordert den Benutzer auf, zur Anmeldeseite zurückzukehren.

Wird von Host Checker ein Ergebnis zurückgegeben, setzt das IVE die Auswertung der Richtlinien auf Bereichsebene fort.

2. **Richtlinien auf Bereichsebene** – Anhand der von Host Checker übermittelten Ergebnisse der ersten Auswertung bestimmt das IVE, auf welche Bereiche der Benutzer zugreifen kann. Anschließend zeigt das IVE Bereiche für den Benutzer an bzw. blendet sie aus. Dieser kann sich nur in den Bereichen anmelden, die für die Anmeldeseite aktiviert sind und deren Anforderungen für Host Checker erfüllt sind. Wenn der Benutzer die Anforderungen von Host Checker für keinen der verfügbaren Bereiche erfüllt, wird die Anmeldeseite nicht angezeigt. Stattdessen wird eine Fehlermeldung angezeigt, die darüber informiert, dass der Benutzer keinen Zugriff hat, es sei denn, Sie konfigurieren Hilfsoptionen, mit Hilfe derer der Benutzer seinen Computer mit den Sicherheitsanforderungen in Einklang bringen kann.

   Überprüfungen auf Bereichsebene erfolgen ausschließlich im Zuge der Anmeldung des Benutzers am IVE. Sollte sich der Systemzustand eines Benutzers während einer Sitzung ändern, bleibt der aktuelle Bereich weiterhin sichtbar, es besteht aber kein Zugriff auf neue Bereiche.

3. **Richtlinien auf Rollenebene** – Nachdem sich der Benutzer an einem Bereich angemeldet hat, wertet das IVE die Richtlinien auf Rollenebene aus und ordnet den Benutzer der Rolle bzw. den Rollen zu, deren Anforderungen für Host Checker erfüllt sind. Anschließend zeigt das IVE die IVE-Startseite an und aktiviert die für die zugeordnete(n) Rolle(n) zulässigen Optionen.

   Wenn Host Checker während einer periodischen Auswertung einen anderen Status zurückgibt, ordnet das IVE basierend auf den neuen Ergebnissen den Benutzer neuen Rollen zu. Wenn der Benutzer während einer periodischen Auswertung die Zugriffsrechte für alle verfügbaren Rollen verliert, beendet das IVE die Sitzung des Benutzers, es sei denn, Sie konfigurieren Hilfsoptionen, mit deren Hilfe der Benutzer seinen Computer mit den Sicherheitsanforderungen in Einklang bringen kann.

Unabhängig vom Ergebnis verbleibt Host Checker auf dem Client. Windows-Benutzer können den Agent manuell deinstallieren, indem sie im Installationsverzeichnis von Host Checker die Datei uninstall.exe ausführen. Wenn Sie die clientseitige Protokollierung über die Seite **System > Log/Monitoring > Client-side Log** aktivieren, enthält dieses Verzeichnis auch eine Protokolldatei, die vom IVE bei jeder Ausführung von Host Checker neu geschrieben wird.

Wenn Sie die dynamische Richtlinienauswertung für Host Checker aktivieren (siehe „Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)“ auf Seite 44), nimmt das IVE bei jeder Änderung des Host Checker-Status eines Benutzers eine Richtlinienauswertung vor. Wenn die dynamische Richtlinienauswertung für Host Checker nicht aktiviert ist, wertet das IVE zwar keine Ressourcenrichtlinien aus, die Authentifizierungsrichtlinie, Rollenzuordnungsregeln und Rolleneinschränkungen werden dennoch bei jeder Änderung des Host Checker-Status eines Benutzers ausgewertet. Konfigurationsanweisungen finden Sie unter „Festlegen von allgemeinen Host Checker-Optionen“ auf Seite 206.

Aufgabenzusammenfassung: Konfigurieren von Host Checker

Gehen Sie zum Konfigurieren von Host Checker folgendermaßen vor:

1. Erstellen Sie Host Checker-Richtlinien, und legen Sie Hilfsoptionen mithilfe der Seite **Signing In > End Point > Host Checker** der Webkonsole fest. Anweisungen hierfür finden Sie unter „Registerkarte „Host Checker““ auf Seite 206.

2. Legen Sie fest, auf welchen Ebenen innerhalb des IVE-Framework Sie die Richtlinien durchsetzen möchten:

   - Um Host Checker-Richtlinien beim ersten Zugriff eines Benutzers auf das IVE zu erzwingen, implementieren Sie die Richtlinien auf Bereichsebene auf der Seite **Users|Administrators > Authentication >** *Ausgewählter Bereich* **> Authentication Policy > Host Checker** der Webkonsole.

   - Um dem Benutzer den Zugriff auf Rollen basierend auf Erfüllung der Host Checker-Richtlinien zu gewähren oder zu verweigern, implementieren Sie die Richtlinien auf Rollenebene mit Hilfe der Seite **Users|Administrators > Roles|Delegation >** *Ausgewählte Rolle* **> General > Restrictions > Host Checker** in der Webkonsole.

   - Um Benutzern Rollen basierend auf Erfüllung der Host Checker-Richtlinien zuzuweisen, verwenden Sie benutzerdefinierte Ausdrücke auf der Seite **Users|Administrators > Authentication >** *Ausgewählter Bereich* **> Role Mapping** in der Webkonsole.

   - Um dem Benutzer den Zugriff auf einzelne Ressourcen basierend auf Erfüllung der Host Checker-Richtlinien zu gewähren oder zu verweigern, verwenden Sie Bedingungen auf der Seite **Resource Policies >** *Ausgewählte Ressource* **>** *Ausgewählte Richtlinie* **> Detailed Rules >** *Ausgewählte|erstellte Regel* der Webkonsole.

   Konfigurationsanweisungen finden Sie unter „Host Checker-Einschränkungen“ auf Seite 423.

3. Legen Sie für Windows-Clients fest, ob zwischen den Clients und dem/den Richtlinienserver(n) oder den Ressourcen Zugriffstunnel für die-Authentifizierungs-Vorabprüfungen erforderlich sind. Anweisungen hierfür finden Sie unter „Festlegen von Host Checker-Tunneldefinitionen für den Zugriff vor der Authentifizierung“ auf Seite 216.

4. Legen Sie fest, auf welche Weise Benutzer auf den Host Checker-Client zugreifen können. Host Checker setzt die definierten Richtlinien mit Hilfe eines clientseitigen Agenten durch.

   - Verwenden Sie zum Aktivieren der automatischen Installation des Host Checker-Clients auf allen Plattformen die Seite **Users|Administrators > Authentication >** *Ausgewählter Bereich* **> Host Checker** der Webkonsole. Konfigurationsanweisungen finden Sie unter „Angeben von Host Checker-Einschränkungen“ auf Seite 423.

- Verwenden Sie zur manuellen Installation von Host Checker auf Windowssystemen die Seite **Maintenance > System > Installers** der Webkonsole, um das Installationsprogramm für Host Checker herunterzuladen. Konfigurationsanweisungen finden Sie unter „Registerkarte „Installers““ auf Seite 361.

5. Legen Sie fest, ob clientseitige Protokolle erstellt werden sollen. Wenn Sie die clientseitige Protokollierung über die Seite **System > Log/Monitoring > Client-side Log** der Webkonsole aktivieren, erstellt das IVE Protokolldateien auf dem System des Benutzers und schreibt bei jeder Ausführung von Host Checker in die Datei. Konfigurationsanweisungen finden Sie unter „Registerkarte „Client-side Logs““ auf Seite 199.

Cache Cleaner – Übersicht

Cache Cleaner ist ein clientseitiger Agent für Windows, der übrig gebliebene Daten wie temporäre Dateien oder Inhalte des Anwendungscache nach einer IVE-Sitzung vom Benutzercomputer entfernt. Wenn sich beispielsweise ein Benutzer von einem Internet-Kiosk beim IVE anmeldet und mit Hilfe eines Browser-Plug-Ins ein Microsoft Word-Dokument öffnet, entfernt Cache Cleaner nach Beenden der Sitzung die im Browsercache (im Ordner „Windows“) gespeicherte temporäre Kopie der Word-Datei. Durch das Entfernen der Kopie verhindert Cache Cleaner, dass andere Benutzer des Kiosks das Word-Dokument suchen und öffnen können, nachdem der IVE-Benutzer seine Sitzung beendet hat.

Cache Cleaner kann zudem Webbrowser daran hindern, die Benutzernamen, Kennwörter und Webadressen dauerhaft zu speichern, die Benutzer in Webformularen eingeben. Vertrauliche Benutzerinformationen werden dadurch nicht auf ungesicherten Systemen gespeichert, da Cache Cleaner verhindert, dass Browser diese Informationen auf unzuverlässige Weise zwischenspeichern.

Weitere Informationen finden Sie unter:

- „Cache Cleaner definieren“ auf Seite 87
- „Cache Cleaner implementieren“ auf Seite 88
- „Cache Cleaner installieren“ auf Seite 89
- „Cache Cleaner ausführen“ auf Seite 90

Cache Cleaner definieren

Wenn Sie Cache Cleaner aktivieren, wird der gesamte über das Modul für die Inhaltsvermittlung des IVE heruntergeladene Inhalt vom Benutzersystem gelöscht. Darüber hinaus können Sie die Einstellungen auf der Seite **Signing In > End Point > Cache Cleaner** der Webkonsole verwenden, um Inhalt von folgenden Speicherorten zu löschen:

- **Definierte Hosts und Domänen** – Wenn ein Benutzer außerhalb des IVE im Internet navigiert, werden Internetdateien in seinem temporären Internetdateiordner gespeichert. Um diese Dateien mit Hilfe von Cache Cleaner zu löschen, müssen Sie den entsprechenden Hostnamen angeben (z. B. www.yahoo.com).

- **Definierte Dateien und Ordner** – Wenn Sie Benutzern auf ihren lokalen Systemen den Zugriff auf Client-Server-Anwendungen gewähren, können Sie Cache Cleaner zum Löschen temporärer Dateien und Ordner, die Anwendungen auf den Systemen der Benutzer erstellen, konfigurieren.

HINWEIS: Wenn Sie Cache Cleaner zum Entfernen von Dateien aus einem Verzeichnis konfigurieren, werden alle Dateien einschließlich jener Dateien gelöscht, die der Benutzer ausdrücklich in diesem Verzeichnis gespeichert hat, sowie Dateien, die sich bereits vor der IVE-Sitzung in diesem Verzeichnis befunden haben.

Cache Cleaner implementieren

Nachdem Sie die zu löschenden Hosts, Domänen, Dateien und Ordner mithilfe der Einstellungen auf der Seite **Signing In > End Point > Cache Cleaner** der Webkonsole festgelegt haben, können Sie den IVE- und Ressourcenzugriff einschränken, indem die Ausführung von Cache Cleaner in den folgenden Komponenten gefordert wird:

- **Richtlinie für die Bereichsauthentifizierung** – Wenn Benutzer versuchen, sich am IVE anzumelden, wertet das IVE die Authentifizierungsrichtlinie des angegebenen Bereichs aus, und es ermittelt, ob für die Authentifizierung auch Cache Cleaner erforderlich ist. In der Konfiguration einer Richtlinie für die Bereichsauthentifizierung können Sie festlegen, dass Cache Cleaner entweder lediglich heruntergeladen wird, dass Cache Cleaner nach dem Herunterladen ausgeführt wird oder dass Cache Cleaner nicht erforderlich ist. Der Benutzer muss sich über einen Computer anmelden, der den für den Bereich festgelegten Cache Cleaner-Anforderungen entspricht. Wenn der Computer des Benutzers die Anforderungen nicht erfüllt, verweigert das IVE dem Benutzer den Zugriff. Sie können Einschränkungen auf Bereichsebene über die Seite **Users > Authentication > [Bereich] > Authentication Policy > Cache Cleaner** in der Webkonsole konfigurieren.

- *Ausgewählter BereichAusgewählte/erstellte Regel***Rolle** – Wenn das IVE ermittelt, welche Rollen einem Administrator oder Benutzer zugeordnet werden können, wertet es die Einschränkungen der einzelnen Rollen aus. Dabei wird festgelegt, ob Cache Cleaner auf der Workstation des Benutzers aktiv sein muss. Wenn dies der Fall ist und Cache Cleaner nicht bereits auf dem Computer des Benutzers aktiv ist, erfolgt keine Rollenzuweisung durch das IVE. Sie können Einschränkungen auf Rollenebene über die Seite **Users > Role > [Rolle] > General > Restrictions > Cache Cleaner** in der Webkonsole konfigurieren.

*Ausgewählte RessourceAusgewählte RichtlinieAusgewählte/erstellte Regel*Sie können festlegen, dass das IVE die Cache Cleaner-Richtlinien nur beim erstmaligen Zugriffsversuch des Benutzers auf den Bereich, die Rolle oder die Ressource auswertet. Als Alternative können Sie über die Einstellungen auf der Registerkarte **Signing In > End Point > Cache Cleaner** angeben, dass das IVE die Richtlinien während der Sitzung des Benutzers in regelmäßigen Abständen erneut auswerten soll. Bei einer periodischen Auswertung ordnet das IVE die Benutzer dynamisch bestimmten Rollen zu und gewährt ihnen je nach den Ergebnissen der letzten Auswertung Zugriff auf neue Ressourcen.

Cache Cleaner installieren

Wenn Sie eine Richtlinie auf einer Bereichs-, Rollen- oder Ressourcenrichtlinienebene implementieren, für die Cache Cleaner erforderlich ist, müssen Sie einen Mechanismus bereitstellen, mit Hilfe dessen das IVE oder der Benutzer Cache Cleaner auf dem Clientcomputer installieren kann. Wenn Sie eine Richtlinie auf einer Bereichs- oder Rollenebene implementieren, für die Cache Cleaner erforderlich ist, müssen Sie einen Mechanismus bereitstellen, mit Hilfe dessen das IVE oder der Benutzer Cache Cleaner auf dem Clientcomputer installieren kann. Andernfalls steht der Cache Cleaner-Client beim Überprüfen der Cache Cleaner-Richtlinie für eine Rückmeldung zum IVE nicht zur Verfügung, so dass dem Computer des Benutzers der Zugriff verweigert wird

Aktivieren Sie die automatische Installation über die Seite **User > Authentication > [Bereich] > Authentication Policy > Cache Cleaner** der Webkonsole, damit das IVE versuchen kann, Cache Cleaner auf dem System des Benutzers zu installieren. In diesem Fall wertet das IVE die Option auf Bereichsebene aus, sobald der Benutzer auf die IVE-Anmeldeseite zugreift, und es überprüft, ob die aktuelle Version von Cache Cleaner auf dem Computer des Benutzers installiert ist. Wenn Cache Cleaner nicht installiert ist, versucht das IVE die Installation mit Hilfe der ActiveX- oder Java-Übertragungsmethode.

Wenn ein Benutzer sich am IVE anmeldet, versucht das IVE, ein ActiveX-Steuerelement auf dem Benutzersystem zu installieren. Wurde das ActiveX-Steuerelement erfolgreich installiert, verwaltet das Steuerelement die Installation von Cache Cleaner.

Wenn das IVE das ActiveX-Steuerelement nicht installieren kann, da Administrator- oder Benutzerberechtigungen fehlen oder ActiveX auf dem Benutzersystem deaktiviert ist, versucht das IVE, Cache Cleaner mit Java zu installieren. Die Java-Übertragungsmethode benötigt nur Benutzerberichtigungen; allerdings muss Java auf dem System des Benutzers aktiviert sein.

Wenn das IVE die Java-Übertragungsmethode nicht verwenden kann, da Java deaktiviert ist, wird der Benutzer über eine Fehlermeldung darüber informiert, dass sein System die Installation von ActiveX oder Java-Anwendungen nicht gestattet und deshalb einige der Zugriffssicherheitsfunktionen nicht ausgeführt werden können.

HINWEIS: Zum Installieren von Cache Cleaner benötigen Benutzer wie unter „Installation von clientseitigen Anwendungen“ auf Seite 411 beschrieben entsprechende Berechtigungen. Wenn dies nicht gegeben ist, müssen Sie zum Umgehen dieser Anforderung den Juniper Installer Service verwenden, der Ihnen auf der Seite **Maintenance > System > Installers** in der Webkonsole zur Verfügung steht.

Cache Cleaner ausführen

Wenn ein Benutzer auf das IVE zugreifen will, stellt das IVE den Status von Cache Cleaner auf dem Clientsystem fest, und es veranlasst die Ausführung der Anwendung mithilfe des folgenden Prozesses:

1. **Erstauswertung** – Wenn ein Benutzer erstmalig auf die IVE-Anmeldeseite zugreifen will, stellt das IVE fest, ob Cache Cleaner auf dem Computer des Benutzers ausgeführt wird. Das IVE führt die Erstauswertung unabhängig davon durch, ob die Cache Cleaner-Richtlinien auf Bereichs-, Rollen- oder Ressourcenrichtlinienebene implementiert wurden.

   Wenn der Benutzer die IVE-Anmeldeseite nach dem Starten von Cache Cleaner und vor dem Anmelden am IVE verlässt, wird Cache Cleaner auf dem Computer des Benutzers ausgeführt, bis der Vorgang durch eine Zeitbegrenzung abgebrochen wird.

   Erhält das IVE von Cache Cleaner aus unbestimmten Gründen (einschließlich nicht eingegebener Benutzeranmeldedaten auf der Anmeldeseite) kein Statusergebnis, zeigt das IVE eine Fehlermeldung an und fordert den Benutzer auf, zur Anmeldeseite zurückzukehren.

   Wird von Cache Cleaner ein Status zurückgegeben, setzt das IVE die Ausführung der Richtlinien auf Bereichsebene fort.

2. **Richtlinien auf Bereichsebene** – Anhand der Ergebnisse der ersten Auswertung bestimmt das IVE, auf welche Bereiche der Benutzer zugreifen kann. Anschließend zeigt das IVE Bereiche für den Benutzer an bzw. blendet sie aus. Dieser kann sich nur in den Bereichen anmelden, die für die Anmeldeseite aktiviert wurden, und für die er die Cache Cleaner-Anforderungen erfüllt. Wenn der Benutzer die Anforderungen von Cache Cleaner für keinen der verfügbaren Bereiche erfüllt, wird die Anmeldeseite nicht angezeigt. Stattdessen wird eine Fehlermeldung mit der Information eingeblendet, dass der Computer der Richtlinie für die Endpunktsicherheit nicht entspricht.

   Überprüfungen für Cache Cleaner auf Bereichsebene erfolgen ausschließlich im Zuge der Anmeldung des Benutzers beim IVE. Sollte sich der Systemzustand eines Benutzers während einer Sitzung ändern, bleibt der aktuelle Bereich weiterhin sichtbar, es besteht aber kein Zugriff auf neue Bereiche.

3. **Richtlinien auf Rollenebene** – Nachdem sich der Benutzer an einem Bereich angemeldet hat, wertet das IVE die Richtlinien auf Rollenebene aus und ordnet den Benutzer den Rollen zu, deren Anforderungen für Cache Cleaner erfüllt sind. Anschließend zeigt das IVE die IVE-Startseite an und aktiviert die für die zugeordnete(n) Rolle(n) zulässigen Optionen.

   Wenn Cache Cleaner während einer periodischen Auswertung einen anderen Status zurückgibt, ordnet das IVE basierend auf den neuen Ergebnissen den Benutzer neuen Rollen zu. Wenn der Endbenutzer während einer periodischen Auswertung die Zugriffsrechte für alle verfügbaren Rollen verliert, beendet das IVE die Sitzung des Benutzers.

4. **Endgültige Bereinigung** – Cache Cleaner führt in folgenden Situationen eine endgültige Bereinigung durch und stellt Registrierungseinstellungen wieder her:

   - **Der Benutzer meldet sich explizit von seiner Benutzersitzung ab** – Wenn ein Benutzer auf der IVE-Startseite auf **Sign Out** klickt, führt Cache Cleaner eine endgültige Bereinigung aus und deinstalliert sich anschließend selbst vom Benutzersystem.

   - **Die Höchstdauer für die Benutzersitzung ist überschritten** – Wenn die Höchstdauer für eine Benutzersitzung überschritten wurde, führt Cache Cleaner eine Bereinigung durch. Meldet sich der Benutzer dann erneut an, wird die Bereinigung wiederholt. Cache Cleaner überprüft in bestimmten Abständen die Gültigkeit einer Sitzung und erkennt daher, wann eine Sitzungszeitüberschreitung auftritt. Die entsprechenden Intervalle werden auf der Registerkarte **Signing In > End Point > Cache Cleaner** festgelegt.

HINWEIS: Bei der Überprüfung der Gültigkeit einer Sitzung stellt Cache Cleaner eine Verbindung mit dem IVE her. Diese Aktion kann die Ausgabe von Warnmeldungen persönlicher Firewalls zur Folge haben. Benutzer müssen diesen Datenverkehr zulassen, damit Cache Cleaner ordnungsgemäß ausgeführt werden kann. Bei Verwendung einer persönlichen Firewall erfolgt bei jedem Leeren des Cache mit Cache Cleaner ein Protokolleintrag.

   - **Ein Clientsystem wird nach einem nicht ordnungsgemäßen Herunterfahren des Systems neu gestartet** – Wenn Cache Cleaner aufgrund eines Problems im System, bei einer Sitzung oder einer Netzwerkverbindung nicht ordnungsgemäß beendet wird, führt Cache Cleaner eine endgültige Bereinigung durch, und deinstalliert sich nach dem Neustart des Systems selbst vom Benutzersystem. Beachten Sie, dass Cache Cleaner nach dem Beenden keine Daten protokollieren kann. Darüber hinaus gehen alle nach dem Beenden und vor der erneuten Anmeldung am IVE vorgenommenen Änderungen der Registrierungseinstellungen des Benutzers verloren.

Unabhängig vom Ausführungsstatus verbleibt Cache Cleaner auf dem Client. Um den Agent manuell zu deinstallieren, kann der Benutzer die Datei uninstall.exe in dem Verzeichnis ausführen, in dem Cache Cleaner installiert ist. Wenn Sie die clientseitige Protokollierung über die Seite **System > Log/Monitoring > Client-side Log** aktivieren, enthält dieses Verzeichnis auch eine Protokolldatei, die bei jeder Ausführung von Cache Cleaner neu geschrieben wird. (Cache Cleaner protokolliert keine Einträge im IVE-Standardprotokoll, kann jedoch Daten in der temporären Client-Textdatei protokollieren. Dieses verschlüsselte Protokoll wird gelöscht, wenn sich Cache Cleaner selbst deinstalliert.)

Weitere Informationen finden Sie unter:

- Weitere Informationen über Verwaltungsoptionen finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 38.

- Weitere Informationen zu Konfigurationsanweisungen für Bereiche, Rollen und Ressourcen finden Sie unter „Cache Cleaner-Einschränkungen“ auf Seite 424.

- Weitere Informationen zu den Verzeichnissen für die Installation, die ausführbare Datei und die Protokolldateien für Cache Cleaner finden Sie unter „Installation von clientseitigen Anwendungen“ auf Seite 411.

Kapitel 4

Remotezugriff

Die Secure Access 700-Appliance ist mit der Network Connect-Zugriffsfunktion ausgestattet, um Benutzern von Remotestandorten aus den einfachen Zugriff auf das IVE zu ermöglichen.

- „Network Connect – Übersicht“ auf Seite 95

Network Connect – Übersicht

Die vom NetScreen-RA 500 verwendete Zugriffsfunktion Network Connect stellt eine clientlose VPN-Verbindung bereit, die als Remotezugriffsmechanismus auf Unternehmensressourcen unter Verwendung einer IVE-Appliance dient. Diese Funktion unterstützt alle Modi für den Internetzugang (einschließlich DFÜ-Verbindungen, Breitband und LAN-Szenarien) vom Clientcomputer aus und funktioniert bei Vorhandensein clientseitiger Proxys und Firewalls, die SSL-Datenverkehr zulassen.

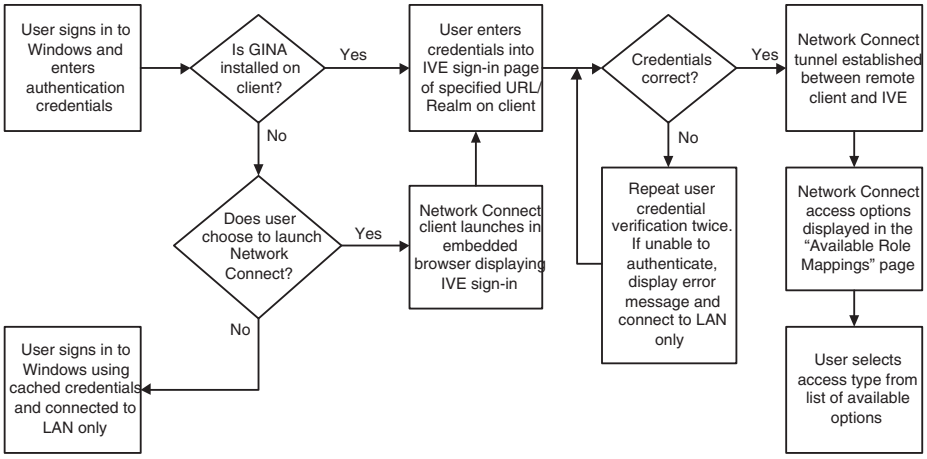
Wenn ein NetScreen-RA 500-Benutzer sich bei einer Network Connect-Sitzung anmeldet und diese startet, wird sämtlicher Datenverkehr an den und vom Client über den sicheren Network Connect-Tunnel übertragen. (Siehe Abbildung 23 auf Seite 96.)

Beim Ausführen von Network Connect wird der Client wie ein Knoten im Remote-LAN (Unternehmens-LAN) behandelt und im lokalen LAN des Benutzers nicht mehr angezeigt. Die IVE-Appliance wird als DNS-Gateway für den Client verwendet und verfügt über keine Informationen zum lokalen LAN des Benutzers. Benutzer können jedoch auf ihrem PC statische Routen festlegen, um bei bestehender Verbindung mit dem Remote-LAN weiterhin auf das lokale LAN zugreifen zu können. Da der gesamte PC-Datenverkehr über den Network Connect-Tunnel zu den internen Unternehmensressourcen übertragen wird, müssen Sie darauf achten, dass andere Hosts im lokalen Netzwerk des Benutzers keine Verbindung mit dem PC herstellen können, auf dem Network Connect ausgeführt wird.

Sie können sicherstellen, dass andere Hosts im lokalen LAN eines Remotebenutzers nicht auf die internen Unternehmensressourcen zugreifen können, indem Sie den Benutzerzugriff auf das lokale Subnetz verweigern (dies wird über die Registerkarte **Users > Roles > [Ausgewählte Rolle] > Network Connect** konfiguriert). Wenn Sie keinen Zugriff auf das lokale Subnetz gewähren, beendet eine IVE-Appliance jene Network Connect-Sitzungen, die von Clients initiiert wurden, auf denen statische Routen festgelegt sind. Sie können festlegen, dass Clients vor dem Starten einer Remotezugriffssitzung auf Netzwerkebene Lösungen für die Endpunktsicherheit ausführen müssen, z. B. eine persönliche Firewall. Mit der Anwendung Host Checker, die Endpunktsicherheitsprüfungen auf Hosts durchführt, die mit einer IVE-Appliance eine Verbindung herstellen, kann sichergestellt werden, dass die Clients Endpunktsicherheitssoftware verwenden. Weitere Informationen finden Sie unter „Host Checker – Übersicht“ auf Seite 75.

Abbildung 23 bietet einen Überblick über die grundlegenden Schritte zur Einrichtung eines Network Connect-Tunnels.

Abbildung 23: Einrichten eines Network Connect-Tunnels


User signs in to Windows and enters authentication credentials
Is GINA installed on client?
Yes
No
User enters credentials into IVE sign-in page of specified URL/ Realm on client
Credentials correct?
Yes
No
Network Connect tunnel established between remote client and IVE
Network Connect access options displayed in the "Available Role Mappings" page
User selects access type from list of available options
Repeat user credential verification twice. If unable to authenticate, display error message and connect to LAN only
Does user choose to launch Network Connect?
Yes
No
Network Connect client launches in embedded browser displaying IVE sign-in
User signs in to Windows using cached credentials and connected to LAN only

Network Connect – Ausführung

HINWEIS: Linux-Benutzer melden sich mit Hilfe des auf der Startseite des sicheren Gateways angezeigten Network Connect-Symbols oder durch Starten von Network Connect per Befehlszeilenschnittstelle bei Network Connect an.

Benutzern, die Network Connect über die Befehlszeilenschnittstelle in X-Windows starten möchten, stehen die folgenden Befehle zur Verfügung:

```
# cd ~/.juniper_networks/network_connect/
# ./ncui -h <Host> -u <Benutzer> -p <Kennwort> [-r <Benutzerbereich>]
```

Benutzer, die Network Connect über eine Befehlszeilenschnittstelle starten möchten, die nicht auf X-Windows basiert, verwenden folgende Befehle:

```
# cd ~/.juniper_networks/network_connect/
# ./ncsvc -h <Host> -u <Benutzer> -p <Kennwort> [-r <Benutzerbereich>]
```

Zum Erstellen einer Verknüpfung auf einem X-Windows Desktop wird killall ncui oder killall ncsvc in das Skript integriert, um beim Beenden von Network Connect sicherzustellen, dass der sichere Tunnel zwischen Client und IVE getrennt wird.

Der Network Connect-Agent wird wie folgt ausgeführt:

1. Ist die automatische Anmeldefunktion „Graphical Identification and Authorization (GINA)“ auf dem Remoteclient installiert und angemeldet, initiiert der Client bei der Anmeldung eines Windows-Benutzers automatisch einen Network Connect-Tunnel zum IVE; ansonsten muss sich der Benutzer beim NetScreen-RA 500 anmelden.

2. Verfügt der Benutzer nicht über die aktuellste Version des Installationsprogramms für Network Connect, versucht die IVE-Appliance, ein ActiveX-Steuerelement (Windows) oder ein Java-Applet (Mac) auf den Clientcomputer herunterzuladen, welches anschließend die Network Connect-Software herunterlädt und die Installation vornimmt. Schlägt der Download oder die Aktualisierung des ActiveX-Steuerelements eines Windows-Clients aufgrund von eingeschränkten Zugriffsrechten oder Browsereinschränkungen fehl, greift die IVE-Appliance zur Übertragung der Network Connect-Software auf ein Java-Applet zurück. Ob das IVE letztendlich ein ActiveX-Steuerelement oder ein Java-Applet herunterlädt, ist ohne Belang. Beide Komponenten versuchen, die Verfügbarkeit und Version von auf dem Client installierter Network Connect-Software zu ermitteln, bevor sie sich für eine der folgenden Installationsarten entscheiden:

   a. Wenn die Network Connect-Software auf dem Client nicht installiert ist, wird die neueste Version installiert.

   b. Ist auf dem Clientcomputer eine ältere Version der Network Connect-Software vorhanden, wird die ältere Version deinstalliert und die neueste Version vom IVE installiert.

HINWEIS: Weiter Informationen über gültige Java-Applets, Installationsdateien und -protokolle sowie Verzeichnisse des Betriebssystems, in denen Übertragungsmechanismen ausgeführt werden, finden Sie unter „Installation von clientseitigen Anwendungen“ auf Seite 411.

---

3. Nach der Installation sendet der clientseitige Network Connect-Agent eine Anforderung an die IVE-Appliance, um die Verbindung mit einer IP-Adresse aus dem zuvor bereitgestellten IP-Pool (entsprechend der Ressourcenrichtlinien für die Network Connect-Verbindungsprofile, die auf die Rolle des Benutzers anwendbar sind) zu initialisieren.

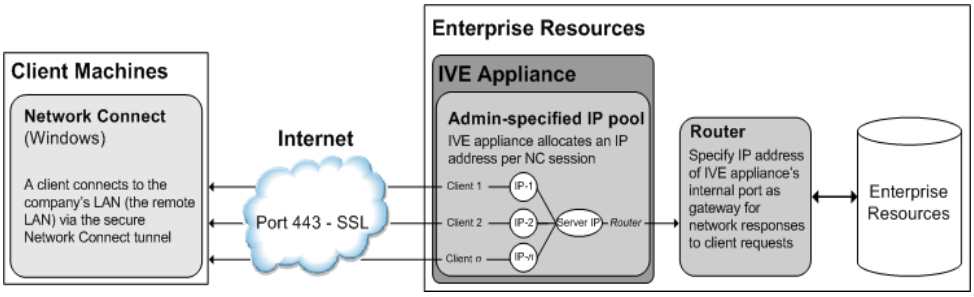
4. Das Network Connect-Symbol befindet sich unter Windows rechts auf der Taskleiste; Auf einem Mac befindet es sich im Dock.

5. Die IVE-Appliance reserviert eine IP-Adresse (von einer Ressourcenrichtlinie für die Network Connect-Verbindungsprofile) und weist dem Network Connect-Dienst auf dem Client eine eindeutige IP zu.

6. Der clientseitige Network Connect-Dienst verwendet die zugewiesenen IP-Adressen für die Kommunikation mit dem in der IVE-Appliance ausgeführten Network Connect-Prozess.

7. Nachdem das IVE dem Client eine IP-Adresse zugeordnet hat, öffnet das IVE einen direkten Kommunikationskanal zwischen dem Client und den Unternehmensressourcen, auf die der Benutzer gemäß den Ressourcenrichtlinien Zugriff hat. Der interne Anwendungsserver erkennt die IP-Quelladresse als die IP-Adresse des Clients.

Abbildung 24: Client/Server-Kommunikation mit Network Connect



Der Client-Agent von Network Connect kommuniziert mit der IVE-Appliance, welche im Gegenzug Benutzeranforderungen an Unternehmensressourcen weiterleitet.

HINWEIS: Wenn Sie Host Checker zur Suche von richtlinienbasierten Client-Sicherheitskomponenten, die mit Hilfe des IVE definiert wurden, einsetzen, und der Benutzer erfüllt die Sicherheitsrichtlinien während einer Network Connect-Sitzung nicht, wird die Sitzung von Host Checker beendet.

Automatische Network Connect-Anmeldung mit „GINA“

Bei der Anmeldefunktion „Graphical Identification and Authorization (GINA)“ handelt es sich um eine automatisierte Anmeldemethode, die Sie zur Anmeldung bei Windows NT-Domänen auf Windows-Clients installieren und aktivieren können. Sie können die Installation von GINA auf Clientrechnern durch Network Connect erzwingen; Sie können aber auch den Benutzer beim Start von Network Connect selbst entscheiden lassen, ob GINA installiert werden soll.

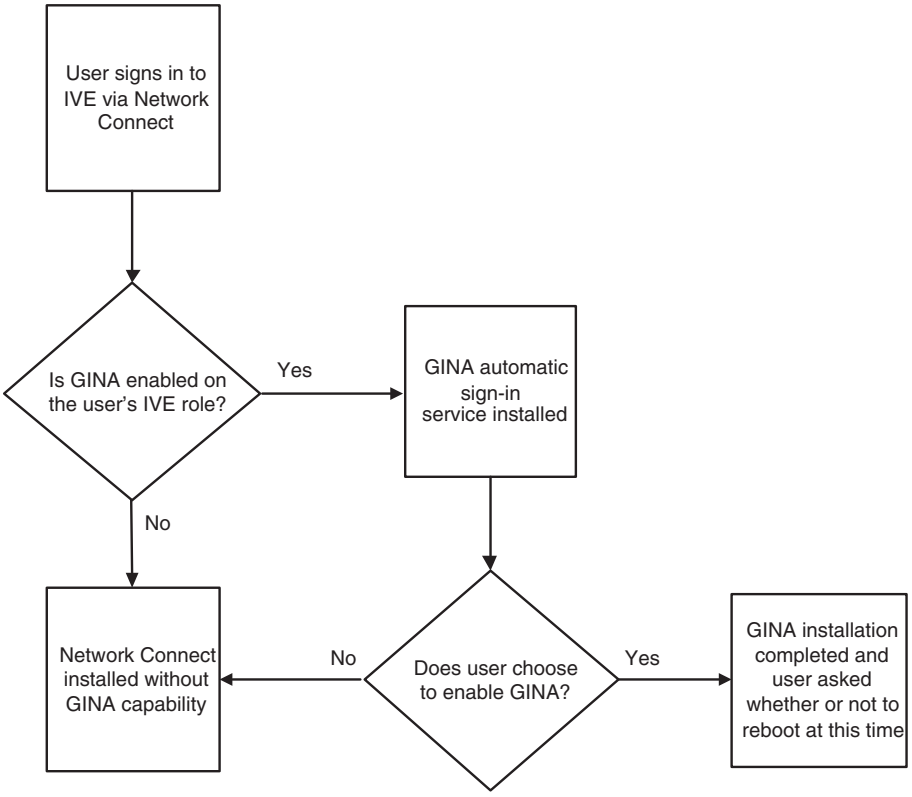
HINWEIS: Pro Clientsystem kann nur eine GINA-Anmeldefunktion installiert werden. Nutzt eine andere Anwendung auf dem Clientsystem bereits eine GINA-Funktion, kann GINA von Network Connect nicht installiert und aktiviert werden.

Ist GINA bereits auf dem Clientsystem installiert, wird vom Benutzer automatisch abgefragt, ob Network Connect bei jeder Windows-Anmeldung gestartet werden soll. Wenn Sie sich für eine optionale GINA-Installation entscheiden, kann GINA vom Benutzer über das Network Connect-Fenster mit Hilfe der Option **Auto connect when login to Windows** aktiviert werden. Diese Option ist nur bei geöffneter Network Connect-Sitzung verfügbar.

Die Option, eine GINA-Installation auf dem Clientsystem zu ermöglichen, steht bei der Definition von Rollenattributen auf der Seite **Users > Roles > [Ausgewählte Rolle] > Network Connect** zur Verfügung. Ausführliche Informationen finden Sie unter „Konfigurieren der Seite „Network Connect““ auf Seite 299.

Abbildung 25 bietet einen Überblick über die grundlegenden Schritte während des GINA-Installationsvorgangs.

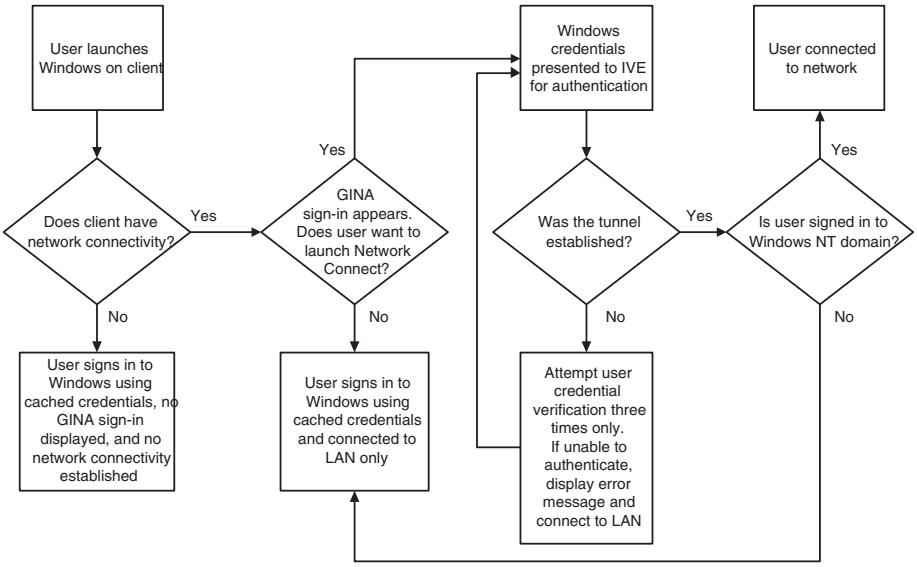
Abbildung 25: GINA-Installationsvorgang


User signs in to IVE via Network Connect
Is GINA enabled on the user's IVE role?
Yes
GINA automatic sign-in service installed
No
Network Connect installed without GINA capability
No
Does user choose to enable GINA?
Yes
GINA installation completed and user asked whether or not to reboot at this time

Der Installationsvorgang von GINA wird einmalig ausgeführt und benötigt einen Systemneustart, um die Anmeldefunktion von GINA zu aktivieren. Ab dieser Sitzung erkundigt sich GINA beim Benutzer, ob Network Connect bei jeder Windows-Anmeldung gestartet werden soll. Wenn sich der Benutzer an Network Connect anmeldet, leitet GINA (sofern nicht anders festgelegt) die Windows-Anmeldeinformationen zur Authentifizierung vor der Initiierung des Network Connect-Tunnels an das IVE weiter.

Abbildung 26 bietet einen Überblick über die grundlegenden Schritte des automatisierten Tunnel-Initiierungsvorgangs von GINA.

Abbildung 26: automatischer Anmeldevorgang von GINA


User launches Windows on client
Does client have network connectivity?
Yes
No
User signs in to Windows using cached credentials, no GINA sign-in displayed, and no network connectivity established
GINA sign-in appears. Does user want to launch Network Connect?
Yes
No
User signs in to Windows using cached credentials and connected to LAN only
Windows credentials presented to IVE for authentication
Was the tunnel established?
Yes
No
Attempt user credential verification three times only. If unable to authenticate, display error message and connect to LAN
Is user signed in to Windows NT domain?
Yes
No
User connected to network

Bereitstellen Ihres Netzwerks für Network Connect

Inkompatibilitäten von Network Connect mit anderen VPN-Clientanwendungen

VPN-Clientanwendungen von Drittanbietern sind mit Network Connect möglicherweise nicht kompatibel. Tabelle 3 zeigt eine Liste von VPN-Clientanbietern und die relative Kompatibilität von Network Connect mit deren Anwendungen.

Tabelle 3: Network Connect-Kompatibilität mit VPN-Clients von Drittanbietern

Anbieter	kompatibel
Cisco	Ja
Nortel	Ja
NS Remote	Ja
Intel	Ja
Checkpoint	Nein

Bei der Installation von Network Connect auf einem Client mit einer inkompatiblen VPN-Clientanwendung muss diese Anwendung vor der Installation oder Ausführung von Network Connect deinstalliert werden.

Clientanforderungen unter Linux

Linux-Clients, die sich bei Network Connect mit Mozilla Firefox 1.6 anmelden, müssen sicherstellen, dass die Bibliotheken OpenSSL und OpenMotif auf dem Client installiert sind. Für den Fall, dass ein Linux-Benutzer nicht über die benötigten OpenSSL- und OpenMotif-Bibliotheken verfügt, stehen diese auf den folgenden Ressourcen kostenlos bereit:

- **OpenSSL** – Die meisten Linux-Versionen sind mit OpenSSL ausgestattet. Ausführliche Informationen erhalten Sie unter http://www.openssl.org/related/binaries.html. (Sie können Benutzer auch anweisen, ihre eigenen Versionen zu kompilieren, indem Sie auf die Quellversion auf http://www.openssl.org/source/ verweisen.) Folgende Version wird benötigt: libssl.so.0.9.6b

- **OpenMotif** – Die Bibliothek OpenMotif kann per FTP über den folgenden Pfad heruntergeladen werden: ftp://openmotif.opengroup.org/pub/openmotif/. Lesen Sie das Dokument *Getting OpenMotif* aufmerksam durch, um Informationen über weitere Anbietersites für diese Bibliothek zu erhalten. Folgende Version wird benötigt: libXm.so.3.0.1

Definieren von Zugriffsmethoden mit Hilfe von Network Connect-Ressourcenrichtlinien

Network Connect-Ressourcenrichtlinien enthalten eine Vielzahl verschiedenster Network Connect-Sitzungsparamenter, mit deren Hilfe Sie die gewünschte Zugriffsmethode für Remoteclients festlegen können. Das IVE bietet Ihnen die folgenden Ressourcenrichtlinientypen zur Konfiguration und zur Anwendung auf eine oder mehrere Benutzerrollen:

- Ressourcenrichtlinien zur Regelung des Zugriffs – Dieser Richtlinientyp bestimmt, auf welche Ressourcen Benutzer bei der Verwendung von Network Connect zugreifen können. Hierzu zählen z. B. Web-, Datei- und Servercomputer des Firmenintranets. Weitere Informationen finden Sie unter „Registerkarte „Network Connect Access Control““ auf Seite 344.

- Ressourcenrichtlinien zur Packet-Protokollierung – Dieser Richtlinientyp ermöglicht die Kompilierung clientseitiger Network Connect-Packet-Protokolle im IVE zur Erkennung und Behebung von Verbindungsproblemen. Weitere Informationen finden Sie unter „Registerkarte „Network Connect Logging““ auf Seite 345.

- Ressourcenrichtlinien für Verbindungsprofile – Dieser Richtlinientyp regelt, welche Option (DHCP oder vom IVE verwalteter IP-Adressen-Pool) das IVE verwendet, um dem Client-Agent von Network Connect eine IP-Adresse zuzuweisen. Diese Funktion kann auch dazu verwendet werden, Transportprotokolle und Verschlüsselungsmethoden für eine Network Connect-Sitzung festzulegen. Weitere Informationen finden Sie unter „Registerkarte „Network Connect Connection Profiles““ auf Seite 346.

- Ressourcenrichtlinien für das Teilen von Tunneln – Dieser Richtlinientyp ermöglicht die Bestimmung mindestens einer Kombination aus IP-Adresse/Netzmaske, deren Datenverkehr zwischen Remoteclient und Firmenintranet über das IVE abgewickelt wird. Weitere Informationen finden Sie unter „Registerkarte „Network Connect Split Tunneling““ auf Seite 350.

Network Connect-Verbindungsprofile mit Unterstützung für mehrere DNS-Einstellungen

Um sicherzustellen, dass Benutzer DNS-Suchen so sicher und effizient wie möglich durchführen können, kann das IVE für multiple DNS-Einstellungen während Network Connect-Sitzungen konfiguriert werden, basierend auf der Rollenmitgliedschaft des jeweiligen Benutzers.

Wenn vom IVE eine Network Connect-Sitzung gestartet wird, kommt für die Sitzung ein entsprechendes Profil zum Einsatz, das auf der Rollenmitgliedschaft des Benutzers basiert und die IP-Adresse, das DNS und die WINS-Einstellungen enthält.

Bei aktivierter Funktion für geteilte Tunnel wird über die Einstellung zur DNS-Suchreihenfolge definiert, welche DNS-Einstellung bevorzugt behandelt wird. Beispiel: Sie suchen nach einem DNS-Server zuerst im Client-LAN und erst danach auf dem DNS-Server des IVE, oder andersherum. Network Connect erstellt vor der Network Connect-Verbindung eine Sicherungskopie der DNS-Einstellungen/-Suchreihenfolge des Clients. Nach dem Sitzungsende stellt Network Connect wieder die ursprünglichen DNS-Einstellungen des Clients her. Wenn die Funktion für geteilte Tunnels deaktiviert wird, werden alle DNS-Anfragen an den DNS-Server des IVE geleitet, und Ihre Einstellung für die DNS-Suchreihenfolge wird nicht angewendet.

Bei Verwendung eines standortübergreifenden Clusters mit mehreren IVEs können der IP-Pool und die DNS-Einstellungen eindeutig dem jeweiligen IVE an den verschiedenen Standorten zugeordnet sein. Aus diesem Grund darf die Richtlinie des Network Connect-Verbindungsprofils knotenspezifisch sein. Das bedeutet, dass die Ressourcenrichtlinie es dem Client ermöglicht, bei jeder neu gestarteten Sitzung innerhalb des Clusters eine Verbindung zum selben IVE herzustellen.

Clientseitige Protokollierung

Bei clientseitigen Network Connect-Protokollen handelt es sich um Dateien, die sich auf dem Remotecomputer befinden und Anmeldungs-, Debug- und andere statistische Informationen beinhalten, mit deren Hilfe mögliche Probleme innerhalb von Network Connect behoben werden können. Ist die clientseitige Protokollierung für Network Connect-Benutzer aktiviert, speichert der Client Network Connect-Ereignisse in einer Reihe von Protokolldateien. Diese werden während einer Benutzersitzung bei jedem Aufruf einer Funktion erweitert. Diese Protokolldateien helfen dem Support-Team bei der Behebung von Problemen in Network Connect. Weitere Informationen finden Sie unter „Festlegen von Einstellungen für clientseitige Protokollierung“ auf Seite 199.

HINWEIS: Wenn Network Connect-Benutzer die clientseitige Protokollierung deaktivieren (auch wenn die Protokollierung auf dem IVE aktiv ist), zeichnet der Client keine clientseitigen Protokollinformationen auf. Wenn der Benutzer die Protokollierungsfunktion aktiviert und das IVE dann zum Deaktivieren der clientseitigen Protokollierung konfiguriert wird, zeichnet der Client keine neuen clientseitigen Protokollinformationen auf.

Network Connect Proxy-Unterstützung

Network Connect bietet Unterstützung für Remoteclients, die mit Hilfe eines Proxyservers auf das Internet (und auf das IVE über das Internet) zugreifen, sowie für Clients, die keinen Proxy für den Internet-Zugriff benötigen, aber mit einem Proxy auf Ressourcen eines internen Netzwerks zugreifen. Network Connect unterstützt auch Clients, die auf eine PAC-Datei (Proxy Automatic Configuration) zugreifen, über die Einstellungen beim Client und beim IVE-Proxy vorgenommen werden, welche den Zugriff auf webbasierte Anwendungen erlauben.

Um diese Proxyanforderungen zu erfüllen, ändert Network Connect die Proxyeinstellungen des Browsers, sodass die temporären Proxyeinstellungen nur für den Datenverkehr der Network Connect-Sitzung verwendet können. Für Datenverkehr, der nicht für die Network Connect-Sitzung bestimmt ist, werden die vorhandenen Proxyeinstellungen verwendet.

Unabhängig von der Aktivierung der Funktion zur Teilung von Tunneln unterstützt das IVE folgende Proxyszenarios:

- Verwenden eines expliziten Proxys für den Zugriff auf das IVE
- Verwenden eines expliziten Proxys für den Zugriff auf interne Anwendungen
- Verwenden einer PAC-Datei für den Zugriff auf das IVE
- Verwenden einer PAC-Datei für den Zugriff auf interne Anwendungen

Wenn geteilte Tunnel im IVE aktiviert sind, werden die Proxyeinstellungen abhängig von der Implementierungsmethode des Proxys auf eine der folgenden Arten von Network Connect verwaltet:

- Für Remoteclients, die einen Proxyserver für den Internet-Zugriff verwenden, werden alle vom Browser erzeugten und für das IVE (einschließlich NCP-Datenverkehr) bestimmten HTTP-Anforderungen entweder über einen expliziten Proxy oder eine PAC-Datei auf der Clientseite geleitet. Da auf Clientseite ein expliziter Proxy bereits vorhanden oder der Zugriff auf eine PAC-Datei bereits möglich ist, richtet der Client vor der dem Start einer Network Connect-Sitzung den lokalen, temporären Proxy ein.
- Bei Remoteclients, die in einem Unternehmensnetzwerk zwar mit Hilfe eines Proxys auf Unternehmensressourcen zugreifen, aber dennoch ohne Proxy eine Internetverbindung herstellen können, stellt Network Connect die Proxyeinstellungen des Clients fest, obwohl der Proxy erst erreichbar ist, wenn Network Connect eine Verbindung herstellt. Nach dem Verbindungsaufbau erstellt Network Connect den lokalen, temporären Proxy.
- Wenn ein Remoteclient auf eine vorkonfigurierte HTTP-basierte PAC-Datei zugreift, kann der Client die PAC-Datei erst abfragen, nachdem Network Connect eine Sitzungsverbindung hergestellt hat. Sobald die Verbindung besteht, greift der Client auf die PAC-Datei zu und fügt deren Inhalt dem lokalen temporären Proxy hinzu. Anschließend werden die Proxyeinstellungen des Browsers aktualisiert.

Aufgabenzusammenfassung: Konfigurieren von Network Connect

In diesem Abschnitt finden Sie Network Connect-Konfigurationsschritte auf höherer Ebene. Diese Schritte wirken sich nicht auf vorher ausgeführte IVE-Konfigurationsschritte aus, wie z. B. das Festlegen der IVE-Netzwerkidentität oder das Hinzufügen von Benutzer-IDs zum IVE.

Gehen Sie zum Konfigurieren des IVE für Network Connect folgendermaßen vor:

1. Ermöglichen Sie den Zugriff auf Network Connect auf der Rollenebene mit Hilfe der Einstellungen auf der Seite **Users > Role > [Ausgewählte Rolle] > General > Overview** in der Webkonsole. Anweisungen hierfür finden Sie unter „Konfigurieren der Seite „General““ auf Seite 277.

2. Erstellen Sie Ressourcenrichtlinien für Network Connect mit Hilfe der Einstellungen auf den Registerkarten von **Resource Policies > Network Connect**:

   a. Legen Sie allgemeine Zugriffseinstellungen und ausführliche Zugriffsregeln für Network Connect auf der Registerkarte **Network Connect Access Control** in der Webkonsole fest. Ausführliche Informationen finden Sie unter „Registerkarte „Network Connect Access Control““ auf Seite 344.

   b. Erstellen Sie Verbindungsprofile für Network Connect, um sie Remotebenutzern zuzuweisen, mit Hilfe der Registerkarte **Network Connect Connection Profiles** in der Webkonsole. Ausführliche Informationen finden Sie unter „Registerkarte „Network Connect Connection Profiles““ auf Seite 346.

   c. (Optional) Erstellen Sie Ressourcenrichtlinien für Network Connect zur Filterung von Packetinformationen über die Registerkarte **Network Connect Logging** in der Webkonsole. Ausführliche Informationen finden Sie unter „Registerkarte „Network Connect Logging““ auf Seite 345.

   d. (Optional) Legen Sie die Einstellungen für getrennte Tunnel in Network Connect mit Hilfe der Registerkarte **Network Connect Split Tunneling** in der Webkonsole fest. Ausführliche Informationen finden Sie unter „Registerkarte „Network Connect Split Tunneling““ auf Seite 350.

3. Bestimmen Sie eine IP-Adresse, die vom Serverprozess von Network Connect für sämtliche Network Connect-Benutzersitzungen verwendet werden soll. Verwenden Sie hierzu die Seite **System > Network > Network Connect** in der Webkonsole. Ausführliche Informationen finden Sie unter „Angeben der IP-Adresse für Network Connect Server“ auf Seite 190.

4. Legen Sie fest, ob die Installation von GINA aktiviert, die Verwendung geteilter Tunnel zugelassen und/oder Network Connect automatisch gestartet werden soll. Die Einstellungen hierfür erfolgen auf der Seite **Users > Role > [Ausgewählte Rolle] > Network Connect** in der Webkonsole. Anweisungen hierfür finden Sie unter „Konfigurieren der Seite „Network Connect““ auf Seite 299.

HINWEIS: Entscheiden Sie sich auf dieser Seite für die Aktivierung der Funktion für geteilte Tunnel, müssen Sie vorher mindestens ein Network Connect-Ressourcenprofil für geteilte Tunnel erstellen, nachzulesen unter Schritt d weiter oben.

5. Stellen Sie gemäß den Anweisungen auf der Registerkarte „Registerkarte „Installers““ auf Seite 361 sicher, dass alle Remoteclients über die passende Version von Network Connect verfügen.

6. (Optional) Legen Sie auf der Seite **System > Log/Monitoring > NC Packet Log** in der Webkonsole fest, ob das IVE Network Connect-Packet-Protokolle für bestimmte Network Connect-Benutzer kompilieren soll. Anweisungen hierfür finden Sie unter „Registerkarten „Events“, „User Access“ „Admin Access“ und „NC Packet““ auf Seite 191.

7. Wenn Sie die clientseitige Protokollierung in Network Connect aktivieren oder deaktivieren wollen, konfigurieren Sie die Optionen der Registerkarte **System > Configuration > Security > Client-side Logs** in der Webkonsole. Anweisungen hierfür finden Sie unter „Festlegen von Einstellungen für clientseitige Protokollierung“ auf Seite 199.

E-Mail-Client – Übersicht

Die vom IVE bereitgestellte E-Mail-Unterstützung hängt von den optionalen Funktionen ab, die für das IVE lizenziert sind:

- **Secure Email Client** – Wenn Sie über die Option Secure Email Client verfügen, unterstützt das IVE IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol).
- **Secure Application Manager** – Wenn Sie über die Option Secure Application Manager verfügen, unterstützt das IVE das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll.

HINWEIS: Wenn das IVE mit der Secure Application Manager-Option lizenziert ist, die das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll unterstützt, trifft dieser Abschnitt nicht zu.

Die Option Secure Email Client bietet Benutzern die Möglichkeit, mit standardbasierten E-Mail-Clients sicher von Remotestandorten auf firmeninterne E-Mail-Nachrichten zuzugreifen, ohne dass weitere Software (z. B. ein VPN-Client) benötigt wird. Das IVE kann mit jedem Mailserver eingesetzt werden, der IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol) unterstützt. Hierzu zählen auch Microsoft Exchange Server und Lotus Notes Mail Server, die IMAP4/POP3/SMTP-Schnittstellen zur Verfügung stellen.

Das IVE befindet sich zwischen dem Remoteclient und dem Mailserver und fungiert als sicherer E-Mail-Proxy. Der Remoteclient verwendet das IVE als (virtuellen) Mailserver und sendet E-Mail-Nachrichten über das SSL-Protokoll. Das IVE beendet SSL-Verbindungen des Clients und leitet den entschlüsselten E-Mail-Verkehr innerhalb des LAN an den Mailserver weiter. Das IVE wandelt den unverschlüsselten Datenverkehr des Mailservers dann in S-IMAP (Secure IMAP)-, S-POP (Secure POP)- und S-SMTP (Secure SMTP)-Datenverkehr um und sendet ihn über SSL an den E-Mail-Client.

Weitere Informationen finden Sie unter:

- „Auswählen eines E-Mail-Clients“ auf Seite 106
- „Arbeiten mit einem standardbasierten Mailserver“ auf Seite 107
- „Arbeiten mit Microsoft Exchange Server“ auf Seite 108
- „Arbeiten mit Lotus Notes und Lotus Notes Mail Server“ auf Seite 110

Auswählen eines E-Mail-Clients

Das IVE unterstützt die folgenden E-Mail-Clients:

- Outlook 2000 und 2002
- Outlook Express 5.5 und 6.x

- Netscape Messenger 4.7x und Netscape Mail 6.2

Benutzer, die Remotezugriff auf E-Mail-Nachrichten benötigen, können normalerweise in zwei Kategorien eingeteilt werden:

- **Laptopbenutzer in der Firma** – Diese Benutzer verwenden im Büro und unterwegs den gleichen Laptop.
- **Benutzer mit Heimcomputern** – Diese Benutzer verwenden zu Hause einen anderen Computer als im Büro.

Bevor Sie Benutzern einen E-Mail-Client empfehlen, sollten Sie die folgenden Abschnitte lesen, in denen erläutert wird, wie die unterstützten Clients mit folgenden Komponenten interagieren:

- Standardbasierte Mailserver wie Lotus Notes Mail Server. Weitere Informationen finden Sie unter „Arbeiten mit einem standardbasierten Mailserver“ auf Seite 107.
- Microsoft Exchange Server. Weitere Informationen finden Sie unter „Arbeiten mit Microsoft Exchange Server“ auf Seite 108.

HINWEIS: Anleitungen zum Konfigurieren der unterstützten E-Mail-Clients finden Sie auf der Supportsite.

Arbeiten mit einem standardbasierten Mailserver

Das IVE kann zusammen mit Mailservern verwendet werden, die IMAP4, POP3 und SMTP unterstützen.

IMAP-Mailserver

- **Laptopbenutzer in der Firma:** Diese Benutzer können jeden der sechs unterstützen E-Mail-Clients verwenden. Wir empfehlen, im Büro und unterwegs den gleichen Client zu verwenden, um übergangsloses Arbeiten zu ermöglichen. Der Client muss dabei so konfiguriert sein, dass er auf das IVE verweist.
- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf den IMAP-Server über das IVE jeden der sechs unterstützten E-Mail-Clients verwenden.

POP-Mailserver

- **Laptopbenutzer in der Firma:** Diese Benutzer können einen der vier Outlook-E-Mail-Clients* verwenden. Wir empfehlen, im Büro und unterwegs den gleichen Client zu verwenden, um übergangsloses Arbeiten zu ermöglichen. Der Client muss dabei so konfiguriert sein, dass er auf das IVE verweist.
- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf den POP-Server über das IVE einen der vier Outlook-E-Mail-Clients* verwenden.

*Die Netscape-E-Mail-Clients können nicht im POP-Modus für den Remotezugriff verwendet werden, da sie S-POP nicht unterstützen. Dieses Protokoll wird jedoch vom IVE für die sichere Datenübertragung gefordert.

Arbeiten mit Microsoft Exchange Server

Microsoft Exchange Server unterstützt:

- Systemeigene MAPI-Clients (Messaging Application Programming Interface)
- IMAP-Clients
- POP-Clients
- Outlook Web Access (OWA)

Das IVE bietet Zugriff auf Microsoft Exchange Server über IMAP- und POP-Clients unter Verwendung der Option für den Secure Email Client und über OWA mit der Funktion für sicheres Webbrowsing.

Wenn Sie den Zugriff auf Microsoft Exchange Server über das systemeigene MAPI-Protokoll ermöglichen möchten, muss das IVE mit der Option für Secure Application Manager lizenziert sein.

Exchange Server und IMAP-Clients

Falls es sich bei dem firmeneigenen Mailserver um Exchange Server handelt, ist der Bürocomputer eines Mitarbeiters wahrscheinlich für die Verwendung des E-Mail-Clients Outlook 2000 oder 2002 im systemeigenen MAPI-Modus konfiguriert.

- **Laptopbenutzer in der Firma:** Diese Benutzer können einen der Outlook Express- oder Netscape-Clients für den Remotezugriff auf Exchange Server über das IVE verwenden.[1]
- **Benutzer mit Heimcomputern:** Diese Benutzer können einen der sechs unterstützten E-Mail-Clients für den Remotezugriff auf Exchange Server über das IVE verwenden, wobei davon ausgegangen wird, dass auf dem Remotecomputer kein MAPI-Konto konfiguriert ist.

1. Der Outlook 2000-Client unterstützt nur eine Mailserverkonfiguration, in diesem Fall den systemeigenen MAPI-Modus. Dies verhindert, dass Benutzer den gleichen Client für den Remotezugriff verwenden. Der Outlook 2002-Client bietet Unterstützung für gleichzeitige MAPI- und IMAP-Serverkonfigurationen. Er unterstützt jedoch den IMAP-Zugriff nicht, wenn das MAPI-Konto offline ist, und verhindert hierdurch, dass Remotebenutzer E-Mail-Nachrichten abrufen können.

Wenn Benutzer die Outlook Express- oder Netscape-Clients im IMAP-Modus ausführen, beachten Sie bitte das folgende Verhalten bei der Ordnerverwaltung:

- **Bei Verwendung von Outlook Express-E-Mail-Clients** – Gelöschte E-Mail-Nachrichten werden im Posteingang von Outlook Express durchgestrichen angezeigt. Sie werden nicht in den Ordner **Gelöschte Objekte** auf dem Exchange Server verschoben, wie es bei Verwendung des Outlook 2000- oder 2002-Clients der Fall ist. Wenn ein Benutzer gelöschte E-Mail-Nachrichten in einem Outlook Express-Client entfernt, werden die E-Mail-Nachrichten endgültig gelöscht. Wir empfehlen Benutzern von Outlook Express die folgende Vorgehensweise:

  - Zu löschende E-Mail-Nachrichten sollten manuell in den unter **Lokale Ordner** angeordneten Ordner **Gelöschte Objekte** verschoben werden (hierbei handelt es sich um Standardordner). Dieser Ordner wird mit dem Ordner **Gelöschte Objekte** auf dem Exchange Server synchronisiert, sodass Benutzer gelöschte E-Mail-Nachrichten später abrufen können.

  - Sie sollten die gelöschten E-Mail-Nachrichten zunächst im Posteingang von Outlook Express lassen und sie dann bei der nächsten Anmeldung bei Outlook 2000 oder 2002 in den Ordner **Gelöschte Objekte** verschieben.

- **Bei Verwendung von Netscape-E-Mail-Clients** – Gelöschte E-Mail-Nachrichten werden in den Ordner **Papierkorb** von Netscape verschoben und im Posteingang von Netscape nicht mehr angezeigt. Aus dem Posteingang von Outlook 2000 oder 2002 werden sie jedoch erst dann entfernt, wenn die Benutzer folgende Schritte ausführen:

  a. Konfigurieren Sie Netscape so, dass gelöschte Nachrichten in den Ordner **Papierkorb** verschoben werden, und aktivieren Sie die Option zum Leeren des Posteingangs bei Beendigung des Programms.

  b. Sie sollten immer nur eines der Programme ausführen und es schließen, wenn Sie Ihre Arbeit beendet haben. Der Posteingang des anderen Programms wird dann mit dem Server synchronisiert, so dass die gleichen Nachrichten angezeigt werden.

  Gesendete E-Mail-Nachrichten werden außerdem in den Netscape-Ordner **Gesendet** (oder einen anderen benutzerdefinierten Ordner) verschoben. Wenn Benutzer möchten, dass gesendete Nachrichten im Ordner **Gesendete Objekte** von Microsoft Exchange Server angezeigt werden, müssen sie sie manuell aus dem Netscape-Ordner für gesendete Objekte in den Ordner **Gesendete Objekte** ziehen.

Exchange Server und POP-Clients

Falls es sich bei dem firmeneigenen Mailserver um Exchange Server handelt, ist der Bürocomputer eines Mitarbeiters wahrscheinlich für die Verwendung des E-Mail-Clients Outlook 2000 oder 2002 im systemeigenen MAPI-Modus konfiguriert.

- **Laptopbenutzer in der Firma:** Diese Benutzer können für den Remotezugriff auf Exchange Server über das IVE einen der unterstützten Outlook Express-Clients verwenden.

- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf Exchange Server über das IVE einen der vier Outlook-Clients verwenden, wobei davon ausgegangen wird, dass auf dem Remotecomputer kein MAPI-Konto konfiguriert ist.

HINWEIS: Die Netscape-E-Mail-Clients können nicht im POP-Modus für den Remotezugriff verwendet werden, da sie S-POP nicht unterstützen. Dieses Protokoll wird jedoch vom IVE für die sichere Datenübertragung gefordert.

Exchange Server und Outlook Web Access

Um auf dem Exchange-Server OWA-Zugriff zur Verfügung zu stellen und es Benutzern zu ermöglichen, über die Webbrowsingfunktion des IVE auf den Exchange-Server zuzugreifen, müssen Sie OWA lediglich im Intranet als Webanwendung bereitstellen. Es ist keine weitere Einrichtung erforderlich, um eine OWA-Implementierung außerhalb des Netzwerks bereitzustellen.

HINWEIS: Bei Verwendung des IVE für den Zugriff auf Outlook Web Access wird der IIS-Webserver für OWA vor Standardangriffen (z. B. Nimda) geschützt und bietet daher erheblich höhere Sicherheit als der Einsatz von OWA direkt über das Internet.

Arbeiten mit Lotus Notes und Lotus Notes Mail Server

Der Lotus Notes Mail Server stellt POP3- und IMAP4-Schnittstellen zur Verfügung, sodass Benutzer E-Mail von einer Lotus Notes-Mailkonfiguration über das IVE abrufen können. Um zu ermitteln, welcher E-Mail-Client sich für die E-Mail-Benutzer im Unternehmen empfiehlt, die Remotezugriff auf den Lotus-Mailserver benötigen, lesen Sie den Abschnitt über die Arbeit mit standardbasierten Mailservern, „Arbeiten mit einem standardbasierten Mailserver“ auf Seite 107.

Aufgabenzusammenfassung: Konfigurieren eines E-Mail-Clients im IVE

So ermöglichen Sie den Zugriff auf:

- **Firmeneigene IMAP-/POP-/SMTP-Mailserver** – Geben Sie Mailserver, E-Mail-Sitzung und Authentifizierungsinformationen auf der Seite **Resource Policies > Email Settings** der Webkonsole an. Weitere Informationen finden Sie unter „Konfigurieren der Seite „Email Client““ auf Seite 354.

Hochladen eines Java-Applets - Übersicht

Die IVE-Funktion zum Hochladen von Java-Applets ermöglicht das Speichern der von Ihnen gewählten Java-Applets direkt im IVE, ohne dass ein separater Webserver zum Hosten eingesetzt wird. Mit dieser Funktion laden Sie die Applets ins IVE hoch und erstellen über das IVE eine einfache Webseite mit Verweisen auf die Applets. Anschließend vermittelt das IVE den Inhalt der Webseite und der Java-Applets mit Hilfe des Moduls für die Inhaltsvermittlung.

Beispiel: Sie möchten mithilfe des IVE Datenverkehr zwischen einem IBM AS/400-System in Ihrem Netzwerk und einzelnen 5250-Terminalemulationen auf den Computern der Benutzer vermitteln. Um das IVE zur Vermittlung dieses Verkehrs zu konfigurieren, ermitteln Sie das Java-Applet der 5250-Terminalemulation. Anschließend laden Sie dieses Applet ins IVE hoch und erstellen eine einfache Webseite, die auf das Applet verweist. Nach dem Erstellen der Webseite über das IVE erstellt das IVE ein entsprechendes Lesezeichen, auf das Benutzer über ihre Startseiten zugreifen können.

HINWEIS: Zur Verwendung dieser Funktion müssen Sie fundierte Kenntnisse über Java-Applets, Java-Applet-Parameter und HTML besitzen.

Dieser Abschnitt enthält die folgenden Informationen über das Hochladen, das Aktivieren und den Zugriff auf Java-Applets über das IVE:

- „Hochladen von Java-Applets in das IVE“ auf Seite 111
- „Signieren von hochgeladenen Java-Applets“ auf Seite 112
- „Erstellen von HTML-Seiten, die auf die hochgeladenen Java-Applets verweisen“ auf Seite 113
- „Zugreifen auf Lesezeichen für Java-Applets“ auf Seite 113
- „Verwendungsbeispiel: Erstellen eines Lesezeichens für ein Java-Applet mit Citrix JICA Version 8.0“ auf Seite 114
- „Aufgabenzusammenfassung: Hochladen und Aktivieren von Java-Applets“ auf Seite 115

Hochladen von Java-Applets in das IVE

Die IVE-Funktion zum Hochladen von Java-Applets ermöglicht das Speichern der von Ihnen gewählten Java-Applets direkt im IVE, ohne dass ein separater Webserver zum Hosten eingesetzt wird. Diese Applets können dann dazu verwendet werden, Verkehr zwischen verschiedenen Arten von Anwendungen über das IVE zu vermitteln. Laden Sie beispielsweise das 3270-Applet, das 5250-Applet oder das Citrix Java-Applet ins IVE hoch. Diese Applets ermöglichen Benutzern das

Einrichten von Sitzungen mit IBM-Mainframes, AS/400-Computern und Citrix MetaFrame-Servern über Terminalemulationen. (Beachten Sie, dass Sie zur Aktivierung des Citrix-Java-ICA-Clients über eine IVE-Sitzung mehrere Citrix-Dateien im Format .jar und .cab ins IVE hochladen müssen. Weitere Informationen hierzu finden Sie unter „Verwendungsbeispiel: Erstellen eines Lesezeichens für ein Java-Applet mit Citrix JICA Version 8.0“ auf Seite 114.)

Das IVE bietet die Möglichkeit, .jar-, .cab-, .zip- und .class-Dateien auf der Seite **Resource Policies > Web > Java > Applets** der Webkonsole hochzuladen. Sie können eine beliebige Anzahl von Java-Applets ins IVE hochladen; die Gesamtgröße darf allerdings 100 MB nicht überschreiten, und jedes Paket muss einen eindeutigen Namen besitzen.

Um die Kompatibilität mit Sun und Microsoft-JVMs (Java Virtual Machines) zu gewährleisten, müssen Sie .jar- und .cab-Dateien ins IVE hochladen.

HINWEIS: Beim Hochladen von Java-Applets ins IVE werden Sie vor dem Abschließen der Installation zum Lesen einer Vereinbarung aufgefordert. Lesen Sie diese Vereinbarung sorgfältig durch. Sie verpflichten sich dazu, die volle Verantwortung für die Rechtmäßigkeit, den Betrieb und den Support der von Ihnen hochgeladenen Applets zu übernehmen.

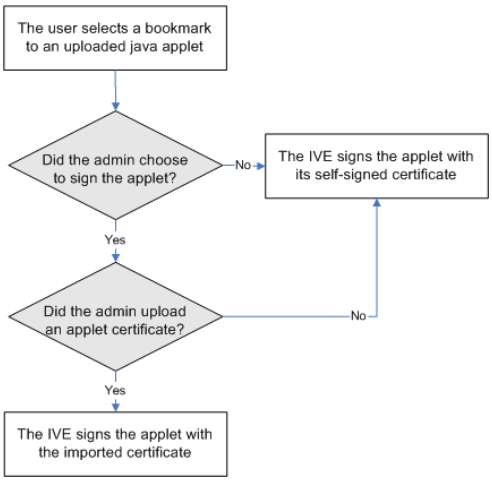
Signieren von hochgeladenen Java-Applets

Im Gegensatz zu anderen Java-Applets, auf die Benutzer über das IVE zugreifen können, müssen Sie für die ins IVE hochgeladenen Java-Applets keine separate Codesignaturrichtlinie erstellen. Das IVE signiert sie automatisch (oder signiert sie neu) unter Verwendung des entsprechenden Codesignaturzertifikats. Bei einem *Codesignaturzertifikat* (auch Appletzertifikat genannt) handelt es sich um ein serverseitiges Zertifikat, das die von einem IVE vermittelten Java-Applets neu signiert. Eine Beschreibung hierzu finden Sie unter „Codesignaturzertifikate“ auf Seite 72.

Ob Sie ein Applet als vertrauenswürdig einstufen, wird durch das Hochladen eines Applets auf der Seite **Resource Policies > Web > Java > Applets** der Webkonsole ausgedrückt. Wenn Sie das Applet als vertrauenswürdig einstufen, signiert (oder signiert neu) das IVE das Applet unter Verwendung des Codesignaturzertifikats, das Sie auf der Seite **System > Configuration > Certificates > Code-signing Certificates** der Webkonsole installieren.

Falls Sie nicht angeben, dass Sie das Applet als vertrauenswürdig einstufen, oder kein Codesignaturzertifikat im IVE installieren, verwendet das IVE zum Signieren oder Neusignieren des Applets ein selbst signiertes Appletzertifikat. In diesem Fall wird den Benutzern immer die Warnmeldung „untrusted certificate issuer“ (nicht vertrauenswürdiger Zertifikataussteller) angezeigt, wenn Sie über das IVE auf das Java-Applet zugreifen.

Abbildung 27: Festlegen, welche Zertifikate beim Signieren von Java-Applets verwendet werden sollen


The user selects a bookmark to an uploaded java applet
Did the admin choose to sign the applet?
No
The IVE signs the applet with its self-signed certificate
Yes
Did the admin upload an applet certificate?
No
Yes
The IVE signs the applet with the imported certificate

Erstellen von HTML-Seiten, die auf die hochgeladenen Java-Applets verweisen

Nach dem Hochladen eines Java-Applets ins IVE müssen Sie zum Erstellen einer einfachen, auf das Applet verweisenden Webseite die Einstellungen auf der Seite **Users > Roles >** *[Rolle]* **> Web > Bookmarks** der Webkonsole verwenden. Die Benutzer können auf diese Webseite über ein Lesezeichen auf den IVE-Startseiten oder von externen Webserver zugreifen (wie beschrieben in „Zugreifen auf Lesezeichen für Java-Applets“ auf Seite 113).

Die Webseite muss eine einfache HTML-Seitendefinition mit Verweis auf das hochgeladene Java-Applet enthalten. Die Webseite kann darüber hinaus zusätzlichen HTML- und JavaScript-Code beinhalten. Das IVE kann einen Teil dieser Webseite für Sie generieren, einschließlich der HTML-Seitendefinition und der Verweise auf das Java-Applet. Beim Generieren dieser Informationen erstellt das IVE Platzhalter für undefinierte Werte und fordert Sie auf, die erforderlichen Werte einzugeben.

Zugreifen auf Lesezeichen für Java-Applets

Die Benutzer können auf die von Ihnen hochgeladenen Applets folgendermaßen zugreifen:

- **Lesezeichen auf der IVE-Endbenutzerkonsole** – Wenn Sie eine Webseite mit Verweisen auf die hochgeladenen Java-Applets erstellen, erstellt das IVE einen entsprechenden Link zu der Webseite und zeigt diesen Link im Abschnitt **Bookmarks** der IVE-Endbenutzerkonsole an. Die der geeigneten Rolle zugeordneten Benutzer können durch Klicken auf den Link auf das Java-Applet zugreifen.

- **Links auf externen Webservern** – Benutzer können unter Verwendung der richtigen URLs von externen Webservern eine Verbindung zu den Lesezeichen für Java-Applets herstellen. Wenn der Benutzer den URL eines Lesezeichens eingibt (oder auf einen externen Link, der den URL enthält, klickt), wird er vom IVE aufgefordert, seinen IVE-Benutzernamen und das Kennwort einzugeben. Ist die Authentifizierung erfolgreich, ermöglicht das IVE den Zugriff auf das Lesezeichen. Sie können den URL für das Lesezeichen für Java-Applets erstellen, indem Sie die Syntax aus einer der folgenden Zeilen verwenden:

  https://<IVE>/dana/home/launchwebapplet.cgi?id=bmname=<bookmarkName>

  https://<IVE>/dana/home/launchwebapplet.cgi?id=<bookmarkID>

  (Legen Sie die ID eines Lesezeichens für Java-Applets fest, indem Sie über die IVE-Startseite darauf zugreifen und die ID dann aus der Adressleiste des Webbrowsers extrahieren.)

HINWEIS: Wenn sich Benutzer am IVE anmelden, um auf ein Lesezeichen für Java-Applets zuzugreifen, müssen sie den von Ihnen auf der Seite **System > Network > Overview** der Webkonsole festgelegten IVE-Hostnamen verwenden. Auf das Lesezeichen oder den URL kann nicht zugegriffen werden, wenn beim Anmelden am IVE die IP-Adresse verwendet wird.

Verwendungsbeispiel: Erstellen eines Lesezeichens für ein Java-Applet mit Citrix JICA Version 8.0

In diesem Abschnitt wird beschrieben, wie unter Verwendung der Java-Version 8.0 des Citrix ICA-Clients (JICA) der Zugriff auf einen Citrix Metaframe-Server über das IVE ermöglicht wird.

So aktivieren Sie den Citrix JICA-Client Version 8.0 unter Verwendung der Java-Applet-Hochladefunktion:

1. Geben Sie einen Hostnamen für das IVE an, und importieren Sie Codesignaturzertifikate. Eine Beschreibung hierzu finden Sie in „Aufgabenzusammenfassung: Hochladen und Aktivieren von Java-Applets“ auf Seite 115.

2. Laden Sie die folgenden .jar- und .cab-Dateien auf der Seite **Resource Policies > Web > Java > Applets** der Webkonsole ins IVE. (Diese Dateien stehen auf der Website von Citrix zur Verfügung.) Geben Sie beim Hochladen dieser Dateien für jede denselben Namen an (z. B. „Citrix JICA 8“):

   - JICA-configN.jar
   - JICA-coreN.jar
   - JICA-configM.cab
   - JICA-coreM.cab

3. Erstellen Sie auf der Seite **Users > Roles >** *[Rolle]* **> Web > Bookmarks** der Webkonsole ein Lesezeichen für Java-Applets. Wählen Sie beim Generieren der Webseite für das Lesezeichen den in Schritt 2 angegebenen Namen in der Liste der Applets aus (z. B. „Citrix JICA 8“). Das IVE fügt nun automatisch alle .jar- und .cab-Dateien in die entsprechende Webseite ein. Geben Sie anschließend Parameter für den Citrix-Client ein. Orientieren Sie sich dabei an den folgenden Beispielen:

```
<html>
<head>
<title>CitrixJICA Applet.</title>
<meta http-equiv="Content-type" content="text/html; charset=ISO-8859-1">
</head>
<body>
 applet code="com.citrix.JICA"
       codebase="<< CODEBASE >>"
       archive="JICA-configN.jar,JICA-coreN.jar"
       width="640" height="480"
       name="CitrixJICA" align="top">
   <param name="code" value="com.citrix.JICA">
   <param name="codebase" value="<< CODEBASE >>">
   <param name="archive" value="JICA-configN.jar,JICA-coreN.jar">
   <param name="cabbase" value="JICA-configM.cab,JICA-coreM.cab">
   <param name="name" value="CitrixJICA">
   <param name="width" value="640">
   <param name="height" value="480">
   <param name="align" value="top">
   <!–
    Geben Sie hier nach dem Kommentar weitere Parameter an.
    <param name="paramname" value="paramvalue">
   –>
   <param name="Address" value="YourMetaFrameServer.YourCompany.net">
    <param name="Username" value="<<USERNAME>>">
   <param name="password" value="<<PASSWORD>>">    <param
name="initialprogram" value="#notepad">
   <param name="EncryptionLevel" value="1">
   <param name="BrowserProtocol" value="HTTPonTCP">
   <param name="End" value="end.html">
 </applet>
</body>
</html>
```

Aufgabenzusammenfassung: Hochladen und Aktivieren von Java-Applets

So erstellen und aktivieren Sie Lesezeichen für Java-Applets im IVE:

1. Geben Sie einen Hostnamen für das IVE auf der Seite **System > Network > Overview** der Webkonsole an. Sie müssen einen Hostnamen angeben, so dass das Java-Applet beim Hochladen ins IVE neu geschrieben werden kann. Anweisungen hierfür finden Sie unter „Konfigurieren allgemeiner Netzwerkeinstellungen“ auf Seite 186.

2. Verwenden Sie zum Hochladen der gewünschten Applets ins IVE die Einstellungen auf der Seite **Resource Policies > Web > Java > Applets** der Webkonsole. Geben Sie beim Hochladen eines Applets an, ob das IVE zum Signieren das Codesignaturzertifikat verwenden soll. Anweisungen hierfür finden Sie unter „Hochladen eines Java-Applets in das IVE“ auf Seite 319.

3. Konfigurieren Sie die entsprechenden Zugriffseinstellungen auf den folgenden Seiten der Webkonsole:

   a. Ermöglichen Sie Benutzern über die Seite **Users > Roles >** [*Rolle*] **> Overview** der Webkonsole den Zugriff auf Webressourcen.

   b. Ermöglichen Sie Benutzern auf der Seite **Users > Roles >** [*Rolle*] **> Overview > der Web console** den Zugriff auf Java-Applets.

   c. Wenn der Zugriff auf eine externe Ressource (z. B. einen Metaframe-Server) erforderlich ist, ermöglichen Sie den Zugriff darauf auf der Seite **Resource Policies > Web > Java > Access Control**.

4. Erstellen Sie mit Hilfe der Einstellungen auf der Seite **Users > Roles >** *[Rolle]* **> Web > Bookmarks** der Webkonsole ein Weblesezeichen mit Verweisen auf die hochgeladenen Applets. Verwenden Sie beim Erstellen des Lesezeichens HTML, um eine Webseite zu erstellen und erforderliche Attribute und Parameter an die Java-Applets zu übergeben. Sie können auch JavaScript und IVE-Variable verwenden. Anweisungen hierfür finden Sie unter „Erstellen von Lesezeichen für Web-URLs“ auf Seite 284.

5. Wenn Sie in Schritt 2 Applets signieren möchten, verwenden Sie zum Hochladen des Javazertifikats ins IVE die Einstellungen auf der Seite **System > Configuration > Certificates > Code-Signing Certificates** der Webkonsole (optional). Wenn Sie diesen Schritt überspringen möchten, wird dem Benutzer jedes Mal beim Zugriff auf das entsprechende Lesezeichen eine Warnmeldung angezeigt, dass es sich um ein nicht vertrauenswürdiges Zertifikat handelt. Anweisungen hierfür finden Sie unter „Importieren eines Codesignaturzertifikats“ auf Seite 181.

Durchgangsproxy – Übersicht

Mit Hilfe der Durchgangsproxy-Funktion können Sie Webanwendungen angeben, für die das IVE eine minimale Vermittlung durchführt. Anders als die herkömmliche Antwortproxyfunktion, bei der ebenfalls nur selektive Teile einer Serverantwort neu geschrieben werden, jedoch sowohl Netzwerkänderungen als auch komplexe Konfigurationen vorgenommen werden müssen, genügt für diese Funktion lediglich die Angabe von Anwendungsserver und Methode, mit der das IVE Clientanforderungen an diese Anwendungsserver empfängt:

- **Über einen IVE-Port** – Wenn Sie eine Anwendung zur Vermittlung für den Durchgangsproxy angeben, geben Sie einen Port an, an dem das IVE Clientanforderungen an den Anwendungsserver abfragen soll. Wenn das IVE eine Clientanforderung für den Anwendungsserver empfängt, leitet es diese Anforderung an den angegebenen Anwendungsserverport weiter. Wenn Sie diese Option auswählen, müssen Sie bei Ihrer Firmenfirewall den Datenverkehr für den angegebenen IVE-Port freigeben.

- **Über virtuellen Hostnamen** – Wenn Sie eine Anwendung zur Vermittlung für den Durchgangsproxy angeben, geben Sie einen Alias für den Hostnamen des Anwendungsservers ein. Für diesen Alias müssen Sie einen Eintrag im externen DNS vornehmen, der für das IVE aufgelöst wird. Wenn das IVE eine Clientanforderung für den Alias empfängt, leitet es diese Anforderung an den für den Anwendungsserver angegebenen Port weiter.

  Diese Option bietet sich an, wenn in Ihrem Unternehmen restriktive Richtlinien für das Öffnen von Firewallports zum Zugriff auf das IVE bestehen. Wenn Sie diese Option verwenden, ist es empfehlenswert, dass jeder Hostnamenalias dieselbe Domänenteilzeichenfolge enthält wie der IVE-Hostname und dass Sie in folgendem Format ein Serverzertifikat mit Platzhalter in das IVE hochladen: *.domaene.de.

  Wenn das IVE beispielsweise iveserver.firmenname.de heißt, muss der Hostnamenalias im Format anwserver.firmenname.de und mit Platzhalter im Format *.firmenname.de angegeben werden. Wenn Sie kein Zertifikat mit Platzhalter verwenden, gibt der Browser eines Clients eine Warnung zu einer Zertifikatsnamenüberprüfung aus, wenn ein Benutzer zu einem Anwendungsserver wechselt, da der Hostnamenalias des Anwendungsservers nicht mit dem Zertifikatsdomänennamen übereinstimmt. Durch dieses Verhalten wird ein Benutzer jedoch nicht daran gehindert, auf den Anwendungsserver zuzugreifen.

Wenn Sie Clientanforderungen an das IVE basierend auf dem Hostnamenalias weiterleiten, müssen Sie das IVE außerdem dem externen DNS-Server hinzufügen. Diese Option bietet sich an, wenn in Ihrem Unternehmen restriktive Richtlinien für das Öffnen von Firewallports für interne Server oder Server in der DMZ gelten.

HINWEIS: Wenn Sie Durchgangsproxys so konfigurieren, dass sie im Modus für virtuelle Hostnamen arbeiten, müssen Benutzer den IVE-Hostnamen verwenden, den Sie bei der Anmeldung beim IVE über die Seite **System > Network > Overview** in der Webkonsole festlegen. Wenn Benutzer bei der Anmeldung beim IVE die IP-Adresse des Durchgangsproxy verwenden, steht ihnen dieser nicht zur Verfügung.

Ebenso wie das eigentliche Vermittlungsmodul bietet die Durchgangsproxy-Option eine höhere Sicherheit als Secure Application Manager, da das IVE dem Client bei Aktivierung für eine Anwendung ermöglicht, an das Firmennetzwerk nur Layer-7-Verkehr an feste Anwendungsports zu senden. Wenn diese Option aktiviert ist, kann das IVE Anwendungen mit Komponenten unterstützen, die nicht mit dem Modul für die Inhaltsvermittlung kompatibel sind, beispielsweise Java-Applets in Anwendungen der Oracle E-Business Suite oder Applets, die auf einer nicht unterstützten Java Virtual Machine ausgeführt werden.

HINWEIS: Die Option des Durchgangsproxy kann nur bei Anwendungen verwendet werden, die feste Ports abfragen und bei denen der Client keine direkten Socketverbindungen herstellt.

Weitere Informationen finden Sie unter:

- „Anwendungsbeispiele für Durchgangsproxys“ auf Seite 118
- „Aufgabenzusammenfassung: Konfigurieren eines Durchgangsproxy“ auf Seite 119

Anwendungsbeispiele für Durchgangsproxys

Wenn das IVE den Namen iveserver.firmenname.de hat und Sie über einen Oracle-Server bei oracle.firmennetzwerk.net:8000 verfügen, können Sie die folgenden Anwendungsparameter bei der Angabe eines IVE-Ports angeben:

Server: oracle.firmennetzwerk.net
Port: 8000
IVE Port: 11000

Wenn das IVE Datenverkehr vom Oracle-Client empfängt, der an iveserver.firmenname.com:11000 gesendet wurde, leitet es den Verkehr an oracle.firmennetzwerk.net:8000 weiter.

Wenn Sie einen Hostnamenalias angeben möchten, können Sie die Anwendung mit folgenden Parametern konfigurieren:

Server: oracle.firmennetzwerk.net
Port: 8000
IVE Alias: oracle.firmenname.de

Wenn das IVE Datenverkehr vom Oracle-Client empfängt, der an oracle.firmenname.de gesendet wurde, leitet es den Datenverkehr an oracle.firmennetzwerk.net:8000 weiter.

Aufgabenzusammenfassung: Konfigurieren eines Durchgangsproxy

Gehen Sie zur Konfiguration eines Durchgangsproxy folgendermaßen vor:

1. Legen Sie die Benutzerrollen fest, denen der Zugriff auf Webanwendungen, die vermittelt werden sollen, gewährt wird. Richten Sie anschließend den Webzugriff dieser Rollen mit Hilfe der Seite **Users > Roles > [Rolle] > General > Overview** in der Webkonsole ein. Anweisungen hierfür finden Sie unter „Verwalten allgemeiner Einstellungen und Optionen für Rollen“ auf Seite 277.

2. Bestimmen Sie Anwendungen, für die das IVE eine minimale Vermittlung durchführt, über die Seite **Resource Policies > Web > Rewriting > Passthrough Proxy** in der Webkonsole. Anweisungen hierfür finden Sie unter „Schreiben einer Ressourcenrichtlinie für Durchgangsproxys“ auf Seite 322.

3. Wenn die Ressourcenrichtlinie für Durchgangsproxys vorsieht, dass das IVE Clientanforderungen über einen IVE-Port empfängt, müssen Sie den ausgewählten Port in der Firmenfirewall für Datenverkehr öffnen. Für den Fall, dass Ihre Richtlinie Anforderungen über einen virtuellen Hostnamen vorsieht:

    a. Hinzufügen einen Eintrags für jeden Hostnamenalias eines Anwendungsservers im externen DNS, der für das IVE aufgelöst wird.

    b. Legen Sie Name und Hostname des IVE auf der Seite **System > Network > Internal Port** in der Webkonsole fest. Anweisungen hierfür finden Sie unter „Konfigurieren allgemeiner Netzwerkeinstellungen“ auf Seite 186.

    c. Laden Sie ein Platzhalterzertifikat über die Seite **System > Configuration > Certificates > IVE Certificates** der Webkonsole auf das IVE hoch. Anweisungen hierfür finden Sie unter „Importieren eines vorhandenen Stammzertifikats und eines privaten Schlüssels“ auf Seite 167.

Kapitel 5

Systemverwaltung und Systemdienste

Das IVE bietet eine Vielzahl von Infrastrukturdiensten, mit deren Hilfe das System verwaltet und individuelle Dienste, wie lokalisierte Versionen des Produkts, wirksam eingesetzt werden können.

Inhalt

Systemverwaltungsfunktionen:

- „Netzwerkeinstellungen – Übersicht“ auf Seite 123
- „Protokollierung und Überwachung – Übersicht“ auf Seite 126
- „Konfigurationsdateien – Übersicht“ auf Seite 129
- „Fehlerbehebung – Übersicht“ auf Seite 144

Systemdienstfunktionen:

- „Unterstützung mehrerer Sprachen – Übersicht“ auf Seite 148

Netzwerkeinstellungen – Übersicht

Das IVE ermöglicht die Änderung der Netzwerkeinstellungen, die bei der erstmaligen IVE-Konfiguration über die serielle Konsole vorgenommenen wurden, sowie die Konfiguration weiterer Netzwerkeinstellungen (z. B. IP-Filter), um andere IVE-Funktionen zu aktivieren. Dieser Abschnitt beinhaltet die folgenden Überblicke über die Netzwerkeinstellungen, die über die Webkonsole des IVE vorgenommen werden:

- „Konfigurieren allgemeiner Netzwerkeinstellungen“ auf Seite 123
- „Konfigurieren interner und externer Ports“ auf Seite 123
- „Konfigurieren von statischen Routen für den Netzwerkverkehr“ auf Seite 124
- „Erstellen von ARP-Zwischenspeichern“ auf Seite 124
- „Angeben von Hostnamen zur lokalen Auflösung durch das IVE“ auf Seite 125
- „Angeben von IP-Filtern“ auf Seite 125

Konfigurieren allgemeiner Netzwerkeinstellungen

Mit Hilfe des IVE können Sie den Status interner und externer Ports anzeigen, einen Hostnamen für das IVE bestimmen und die DNS-Namensauflösung, Windows Internet Naming Service-(WINS)-Server sowie Einstellungen des Masterbrowsers des IVE über die Einstellungen der Seite **System > Network > Overview** in der Webkonsole konfigurieren. Mit den Einstellungen auf dieser Seite können Sie auch die DNS- und WINS-Einstellungen anzeigen, die Sie über die serielle Konsole bei der erstmaligen Installation vorgenommen haben.

Konfigurieren interner und externer Ports

Über den internen Port (auch interne Schnittstelle genannt) werden alle WAN- und LAN-Anforderungen an sämtliche Ressourcen abgewickelt, also u. a. Authentifizierungsanforderungen. Die Konfiguration des internen Ports erfolgt durch die Bereitstellung von IP-Adresse, Gateway, DNS-Server und -Domäne sowie MTU-Einstellungen bei der Ersteinrichtung des IVE. Diese Einstellungen können über die Registerkarte **System > Network > Internal Port > Settings** auch geändert werden. Weitere Informationen finden Sie unter „Registerkarten „Internal Port““ auf Seite 187. (Sie können die Appliance auch im Dual-Port-Modus bereitstellen, um eingehende Verbindungen an einem externen Port abzufragen, wie unter „Registerkarten „External Port““ auf Seite 188 beschrieben.)

Über den externen Port (auch externe Schnittstelle genannt), werden alle Anforderungen von Benutzern abgewickelt, die von außerhalb des Kunden-LAN am IVE angemeldet sind, z. B. über das Internet. Vor dem Senden eines Pakets ermittelt das IVE, ob das Paket einer TCP-Verbindung zugeordnet ist, die von einem Benutzer über die externe Schnittstelle initiiert wurde. Ist dies der Fall, sendet das IVE das Paket an die externe Schnittstelle. Alle übrigen Pakete werden an die interne Schnittstelle gesendet.

Die für jede Schnittstelle festgelegten Routen werden verwendet, nachdem das IVE ermittelt hat, ob die interne oder die externe Schnittstelle zu verwenden ist. Das IVE leitet keine Anforderungen von der externen Schnittstelle ein, und diese Schnittstelle akzeptiert keine anderen Verbindungen (mit Ausnahme von Ping- und Traceroutеverbindungen). Alle Anforderungen an eine beliebige Ressource werden von der internen Schnittstelle ausgegeben. (Weitere Informationen finden Sie unter „Konfigurieren allgemeiner Netzwerkeinstellungen“ auf Seite 123.)

HINWEIS: Wenn Sie den externen Port aktivieren, können sich Administratoren standardmäßig nicht mehr von einem externen Standort aus anmelden. Sie können den externen Port für Administratoren über die Registerkarte **Administrators > Authentication >** *Bereichname* **> Authentication Policy > Source IP** öffnen. Weitere Informationen finden Sie unter „Quell-IP-Zugriffseinschränkungen“ auf Seite 46.

Konfigurieren von statischen Routen für den Netzwerkverkehr

Das IVE ermöglicht Ihnen das Hinzufügen von Einträgen zur Routingtabelle über die Registerkarte **System > Network > Routes**. Alle Verbindungsanforderungen an interne Ressourcen erfolgen vom internen IVE-Port aus, unabhängig von den Routeneinstellungen. Die Routeneinstellungen des externen Ports werden nur zur Weiterleitung von Paketen verwendet, welche Verbindungen zugeordnet sind, die von einem Remoteclient initiiert wurden.

Wenn Sie möchten, dass das IVE beim Routen von Anforderungen eine bestimmte Route nutzen soll, können Sie statische Routen hinzufügen. Hierfür geben Sie gültige IP-Adresse, Gateway sowie DNS-Adresse an. Mit Hilfe der Metrik können mehrere Routen verglichen werden, um Prioritäten festzulegen. Im Allgemeinen gilt: Je niedriger die Zahl (von 1 bis 15), desto höher die Priorität. Eine Route mit dem Metrikwert 2 hat also Vorrang vor einer Route mit dem Metrikwert 14. Der Metrikwert null (0) kennzeichnet eine Route, die nicht genutzt werden sollte.

Erstellen von ARP-Zwischenspeichern

Mithilfe der ARP-Zwischenspeicherung können Sie die physische Adresse (MAC-Adresse) eines Netzwerkgeräts (z. B. eines Routers oder Backend-Anwendungsservers) ermitteln, das eine Verbindung mit dem IVE herstellt. Verwenden Sie die Registerkarte **System > Network > Internal Port > ARP Cache**, um folgende Typen von ARP-Einträgen (Address Resolution Protocol) zu verwalten:

- **Statische Einträge** – Sie können dem Cache, der der IP- und MAC-Adresse zugeordnet ist, einen statischen ARP-Eintrag hinzufügen. Das IVE speichert statische Einträge während eines Neustarts und reaktiviert sie nach dem Neustart. Statische Einträge sind immer auf dem IVE verfügbar.

- **Dynamische Einträge** – Das Netzwerk „erlernt“ dynamische ARP-Einträge während der regulären Verwendung und Interaktion mit anderen Netzwerkgeräten. Die dynamischen Einträge werden vom IVE bis zu 20 Minuten zwischengespeichert und bei einem Neustart gelöscht. Sie haben auch die Möglichkeit, die dynamischen Einträge manuell zu löschen.

Sie können statische und dynamische Einträge aus dem ARP-Cache anzeigen und löschen sowie statische Einträge hinzufügen. Wenn Sie über einen Cluster von IVEs verfügen, sollten Sie beachten, dass ARP-Cacheinformationen knotenspezifisch sind. Das IVE synchronisiert ARP-Cacheinformationen nur innerhalb von Clustern, die nicht über mehrere Sites verfügen.

Angeben von Hostnamen zur lokalen Auflösung durch das IVE

Geben Sie auf der Registerkarte **Hosts** Hostnamen an, die vom IVE lokal zu IP-Adressen aufgelöst werden können. Diese Funktion bietet sich in folgenden Fällen an:

- Das IVE kann nicht auf den DNS-Server zugreifen
- Im LAN wird über WINS auf Server zugegriffen
- Die Sicherheitsrichtlinien Ihres Unternehmens lassen die Auflistung interner Server auf einem externen DNS nicht zu oder erfordern die Maskierung interner Hostnamen

Angeben von IP-Filtern

Über die Registerkarte **Network Connect** können IP-Filter für das IVE angegeben werden, die von diesem auf die IP-Pools von Network Connect angewendet werden. Bei einem IP-Pool handelt es sich um einen festgelegten IP-Adressenbereich, der für Anforderungen von Network Connect zur Verfügung steht. Weitere Informationen finden Sie unter „Network Connect – Übersicht“ auf Seite 95.

Protokollierung und Überwachung – Übersicht

IVE-Protokolldateien sind auf der IVE gespeicherte Dateien, die zur Verfolgung von Systemereignissen dienen. Eine IVE-Appliance generiert vier Arten von Protokolldateien:

- **Events log** – Diese Protokolldatei enthält eine Reihe von Systemereignissen, wie Sitzungsabläufe (z. B. aufgrund von Leerlauf oder Überschreitung der Sitzungshöchstdauer), Systemfehler und -warnungen, Anforderungen zur Überprüfung der Serververbindung und Benachrichtigungen über einen Neustart des IVE-Dienstes. (Der IVE-Überwachungsprozess prüft in regelmäßigen Abständen den IVE-Server und startet ihn neu, falls das IVE nicht reagiert.)

- **User Access log**– Diese Protokolldatei enthält Informationen über Benutzerzugriffe auf die Appliance, einschließlich der Anzahl gleichzeitig angemeldeter Benutzer jeweils nach Ablauf einer Stunde (Anmeldung zur vollen Stunde), Benutzeran- und -abmeldungen, Dateianforderungen durch Benutzer.

- **Administrator Access log**– Diese Protokolldatei enthält Administratorinformationen, einschließlich Änderungen des Administrators an den Benutzer-, System- und Netzwerkeinstellungen, z. B. Änderungen an der Sitzungshöchstdauer sowie Geräte- und Serverinformationen. Außerdem wird bei jeder Anmeldung, Abmeldung oder Änderung von Lizenzen auf der Appliance durch einen Administrator ein Protokolleintrag erstellt.

- **Network Connect Packet log** – Diese Protokolldatei enthält alle im Benutzerzugriffsprotokoll enthaltenen Informationen. Außerdem enthält sie zusätzliche Informationen, wie z. B. die IP-Quell- und -Zieladressen, Quell- und Zielports, UDP-encapsulated Aushandlungsereignisse für das ESP-Transportprotokoll und das Zielprotokoll, das verwendet wird, wenn auf Anwendungen über den Network Connect-Client-zu-IVE-Tunnel zugegriffen wird.

HINWEIS: Da die clientseitige Network Connect-Paketprotokollierung richtliniengesteuert ist, werden Paketinformationen nur für die Benutzerprofile protokolliert, die alle für die automatische Verwendung der Protokollierungsfunktion erforderlichen Kriterien erfüllen.

Auf den Seiten **System > Log/Monitoring** können Sie angeben, welche Ereignisse protokolliert werden, die maximale Dateigröße für das Systemprotokoll festlegen und einstellen, ob Ereignisse zusätzlich zur lokalen Protokollierung auch auf dem Syslog-Server protokolliert werden sollen. Auf den Seiten **System > Log/Monitoring** können Sie die angegebene Anzahl von Ereignissen anzeigen, die Protokolldatei im Netzwerk speichern und den Inhalt der Protokolle löschen.

Wenn eines der Protokolle die konfigurierte maximale Dateigröße (standardmäßig 200 MB) erreicht, werden die aktuellen Daten in eine Sicherungsprotokolldatei verschoben. Dann wird eine neue, leere Datei für alle folgenden (neuen) Protokollmeldungen erstellt. Mithilfe des Protokollbetrachters kann der Administrator die letzten 5000 Protokollmeldungen (Anzeigebeschränkung des Betrachters) anzeigen. Wenn die aktuelle Protokolldatei weniger als 5000 Protokollmeldungen enthält, werden ältere Protokollmeldungen aus der Sicherungsprotokolldatei geöffnet, so dass insgesamt 5000 Protokollmeldungen angezeigt werden. Dabei werden die Protokolldateien wie eine einzige Datei angezeigt, obwohl sie aufgrund der konfigurierten maximalen Dateigröße getrennt gespeichert sind.

HINWEIS: Wenn Sie die Protokollmeldungen speichern oder die FTP-Archivierungsfunktion auf der Seite **Maintenance > Archiving** verwenden möchten, wird die Sicherungsprotokolldatei an die aktuelle Protokolldatei angehängt, und beide werden anschließend als eine Protokolldatei heruntergeladen. Wenn die Protokolldateien nicht archiviert oder gespeichert werden, gehen die ältesten Protokollmeldungen (in der Sicherungsprotokolldatei gespeichert) beim nächsten Verschieben der aktuellen Protokolldatei in die Sicherungsprotokolldatei verloren.

Außerdem können Sie eine IVE-Appliance mit einem Netzwerkverwaltungstool wie HP OpenView als SNMP-Agent überwachen. Die IVE-Plattform unterstützt SNMP v2, implementiert eine private MIB (Management Information Base) und definiert eigene Traps. Um die Verarbeitung dieser Traps in der Netzwerkverwaltungsstation zu ermöglichen, müssen Sie die Juniper Networks-MIB-Datei herunterladen und die entsprechenden Angaben zum Empfangen der Traps machen. Einige der Traps können nach eigenen Anforderungen konfiguriert werden. Weitere Informationen zum Definieren von Trap-Grenzwerten finden Sie unter „Registerkarte „SNMP““ auf Seite 193.

HINWEIS: Zum Überwachen wesentlicher Systemstatistiken, beispielsweise der CPU-Auslastung, laden Sie die UC-Davis-MIB-Datei in Ihre SNMP-Managementanwendung. Sie erhalten die MIB-Datei im Internet unter folgender Adresse: http://net-snmp.sourceforge.net/docs/mibs/UCD-SNMP-MIB.txt.

In den Protokolldateien für Ereignisse, Benutzerzugriff und Administratorzugriff werden die Ereignisse anhand der folgenden Richtlinien hierarchisiert:

- **Critical (Sicherheitsstufe 10)** – Wenn das IVE Benutzer- und Administratoranforderungen nicht bedienen kann oder seine Funktionen für einen Großteil der Untersysteme verliert, wird ein kritisches Ereignis („Critical Event“) protokolliert.

- **Major (Sicherheitsstufe 8-9)** – Wenn das IVE seine Funktionen in mindestens einem Untersystem verliert, aber noch auf die Appliance für andere Zugangsmechanismen zugreifen kann, wird ein größeres Ereignis („Major Event“) protokolliert.

- **Minor (Sicherheitsstufe 5-7)** – Wenn das IVE einen Fehler findet, der keinem größeren Ausfall in einem Untersystem entspricht, wird ein kleineres Ereignis („Minor Event“) protokolliert. Kleinere Ereignisse entsprechen üblicherweise einzelnen fehlgeschlagenen Anforderungen.

- **Info (Sicherheitsstufe 1-4)** – Wenn das IVE eine Benachrichtigungsmeldung anzeigt, wenn ein Benutzer eine Anforderung vornimmt oder ein Administrator eine Änderung durchführt, wird ein Informationsereignis („Informational Event“) protokolliert.

Konfigurationsdateien – Übersicht

Das IVE bietet unterschiedliche Methoden zum Sichern und Wiederherstellen von Konfigurationsdateien, die Benutzer- und Systemdaten enthalten. Die zum Sichern und Wiederherstellen von Daten verfügbaren IVE-Dienstprogramme speichern die Konfigurationsdaten in zwei unterschiedlichen Formaten: binär und XML. Die zu verwendende Methode richtet sich nach Ihren Anforderungen.

Mit IVE-Verwaltungsfunktionen für Konfigurationsdateien können Sie Dateien wie in den folgenden Abschnitten beschrieben importieren, exportieren, speichern und archivieren:

- „Archivieren von IVE-Konfigurationsdateien“ auf Seite 129
- „Importieren und Exportieren von IVE-Konfigurationsdateien“ auf Seite 130
- „Importieren und Exportieren von XML-Konfigurationsdateien“ auf Seite 130
- „Strategien für die Arbeit mit XML-Instanzen“ auf Seite 142

Archivieren von IVE-Konfigurationsdateien

Das IVE ermöglicht Ihnen die Verwendung von SCP (Secure Copy) oder FTP für die tägliche oder wöchentliche automatische Archivierung einer binären Kopie Ihrer Systemprotokolle, Konfigurationsdateien und Benutzerkonten. Das IVE verschlüsselt die Konfigurationsdateien und Benutzerkonten, um eine sichere Übertragung und sichere Speicherung auf anderen Servern zu gewährleisten, und archiviert die Dateien dann entsprechend Ihren Datums- und Uhrzeiteinstellungen im angegebenen Server und Verzeichnis.

SCP ist ein mit FTP vergleichbares Dateiübertragungsprogramm. SCP verschlüsselt alle Daten während der Übertragung. Wenn die Daten ihr Ziel erreichen, werden sie im ursprünglichen Format dargestellt. SCP ist in den meisten SSH-Versionen enthalten und auf allen gängigen Betriebssystemplattformen verfügbar.

Der Name der Archivdateien enthält, wie nachfolgend dargestellt, das Datum und die Uhrzeit der Archivierung:

- Systemereignisse: JuniperAccessLog-*Hostname-Datum-Zeit*
- Benutzereignisse: JuniperEventsLog-*Hostname-Datum-Zeit*
- Administratorereignisse: JuniperAdminLog-*Hostname-Datum-Zeit*
- Systemkonfigurationsdateien: JuniperConf-*Hostname-Datum-Zeit*
- Benutzerkonten: JuniperUserAccounts-*Hostname-Datum-Zeit*

Die Archivierung kann über die Seite **Maintenance > Archiving > FTP Archiving** der Webkonsole aktiviert werden. Anweisungen hierfür finden Sie unter „Registerkarte „FTP Server““ auf Seite 376.

Importieren und Exportieren von IVE-Konfigurationsdateien

Das IVE ermöglicht Ihnen das Importieren und Exportieren von IVE-Systemeinstellungen und -Netzwerkeinstellungen mithilfe von binären IVE-Konfigurationsdateien. Beim Importieren einer Systemkonfigurationsdatei können Sie das Serverzertifikat und die IP-Adresse oder die Netzwerkeinstellungen des IVE-Servers aus den importierten Informationen ausschließen. Wenn Sie z. B. mehrere IVEs hinter einem Load-Balancer einrichten möchten, importieren Sie alle Daten außer der IP-Adresse. Um ein IVE als Sicherungsserver einzurichten, importieren Sie alle Daten außer dem digitalen Zertifikat und den Netzwerkeinstellungen.

HINWEIS:

- Beim Importieren einer Konfigurationsdatei mit Lizenzen erhalten im IVE die bestehenden Lizenzen Vorrang, die gegenwärtig auf dem IVE installiert sind. Archivierte Lizenzen werden nur importiert, wenn auf dem IVE gegenwärtig keine Lizenzen vorhanden sind.

- Beim Importieren von Zertifikaten importiert das IVE nur Serverzertifikate und nicht die Ketten, die IVE-Serverzertifikaten oder vertrauten Clientzertifizierungsstellen entsprechen.

Das IVE ermöglicht Ihnen auch das Importieren und Exportieren aller für lokale Authentifizierungsserver definierten lokalen Benutzerkonten.

HINWEIS: Wenn Sie Ressourcenrichtlinien exportieren möchten, müssen Sie nicht die Systemeinstellungen exportieren, sondern die Benutzereinstellungen. Ressourcenrichtlinien können über die Registerkarte **Maintenance > Import/Export > Import/Export Users** exportiert werden.

Aufgabenzusammenfassung: Importieren und Exportieren von Konfigurationsdateien und Benutzerkonten

1. Verwenden Sie die Einstellungen auf der Seite **Maintenance > Import/Export > Configuration** der Webkonsole, um System- und Netzwerkeinstellungen zu importieren und zu exportieren. Anweisungen hierfür finden Sie unter „Registerkarte „Configuration““ auf Seite 364.

2. Verwenden Sie die Einstellungen auf der Seite **Maintenance > Import/Export > User Accounts** der Webkonsole, um lokale Benutzerkonten zu importieren und zu exportieren. Anweisungen hierfür finden Sie unter „Registerkarte „User Accounts““ auf Seite 365.

Importieren und Exportieren von XML-Konfigurationsdateien

Die Funktion **XML Import/Export** ermöglicht die Durchführung erheblicher Änderungen der Systemkonfiguration und bietet insbesondere im Zusammenhang mit umfangreichen wiederholten Änderungen oder dem gleichzeitigen Hinzufügen, Aktualisieren und Löschen aller Konfigurationsdaten eine Reihe von Vorteilen.

Folgende Aufgaben können u. an. mithilfe von exportierten XML-Konfigurationsdateien ausgeführt werden:

- Hinzufügen einer großen Anzahl von Benutzer
- Löschen aller oder vieler Authentifizierungsserver, Benutzer oder anderer IVE-Objekte
- Verfolgen von Konfigurationsänderungen durch den Vergleich wöchentlicher Exporte
- Ändern mehrerer Instanzen einer Einstellung, z. B. eines Authentifizierungsservernamens
- Erstellen einer Konfigurationsvorlage für die Einrichtung neuer IVE-Appliances

HINWEIS: XML-Instanzdateien können nur zwischen IVEs mit der gleichen Version der IVE-Systemsoftware exportiert und importiert werden. Die Funktion **XML Import/Export** kann nicht verwendet werden, um eine ältere Produktversion mit den aus einer neuen Produktversion exportierten Konfigurationsdateien zu aktualisieren. Eine neuere Produktversion kann auch nicht mit den aus einer älteren Produktversion exportierten Konfigurationsdateien auf eine ältere Version heruntergestuft werden.

Das IVE ermöglicht den Export mehrerer Konfigurationsdatentypen. Hierzu zählen einige Netzwerkeinstellungen, Anmeldeeinstellungen, Authentifizierungsserver, Bereiche, Rollen, Ressourcenrichtlinien und Benutzer. Diese Einstellungen können anschließend in dasselbe oder ein anderes IVE importiert werden.

Sie können XML-Konfigurationsdateien mit den Einstellungen in der folgenden Liste exportieren. Darüber hinaus sind möglicherweise weitere Einstellungen verfügbar.

- **Netzwerkeinstellungen** – Network Connect-Server-IP-Adresse, DNS-Server, DNS-Domänen, Hosts, NICs, NIC-IDs, Quell-IP-Aliase, ARP-Cache, Zeitüberschreitung für ARP-Ping, Standardgateway, IP-Adresse, MTU, NIC-Name, Netzmaske, statische Routen, Verbindungsgeschwindigkeit, NIC-Typ, Hostname und WINS-Adresse.

HINWEIS: Die beiden NIC-IDs in der XML-Instanzdatei dürfen niemals geändert werden. Das IVE geht immer davon aus, dass jede Appliance über zwei Schnittstellenkarten verfügt: NIC0 und NIC1.

Die IDs werden in den NIC-Elementen <sys:NICIdentifier>0</sys:NICIdentifier> und <sys:NICIdentifier>1</sys:NICIdentifier> angezeigt.

- **Anmeldeeinstellungen** – Authentifizierungsserver, Kennwortoptionen, Kennwortverwaltungsoptionen, Standardanmeldeseiten, benutzerdefinierter Text, Headeroptionen, benutzerdefinierte Fehlermeldungen, Hilfeoptionen, Seitenname und Seitentyp.

HINWEIS: Sie können nur Standardanmeldeseiten exportieren. Benutzerdefinierte Anmeldeseiten können nicht exportiert werden.

- **Authentifizierungsbereiche** – Benutzer- und Administratorbereiche, Bereichsnamen, Bereichstypen, Einstellungen für den primären und sekundären Server, Einstellungen für die dynamische Richtlinienauswertung, Authentifizierungsrichtlinien, Grenzwerte, Kennwortrichtlinien, Rollenzuordnungseinstellungen und Rollenverarbeitungsoptionen.

- **Rollen** – Benutzerrollen, Administratorrollen, Rollennamen, aktivierte Funktionen, Einschränkungen, Sitzungsoptionen, Benutzeroberflächenoptionen, Windows- und UNIX-Dateieinstellungen, Weboptionen, Network Connect-Optionen, Telnet-Optionen, Administratorsystemoptionen, Ressourcenrichtlinieneinstellungen und Authentifizierungsbereicheinstellungen.

- **Ressourcenrichtlinien** – Network Connect-Zugriffsrichtlinienlisten, Richtlinienlisten für das selektive Neuschreiben von Webinhalten, Richtlinien für das selektive Neuschreiben von Webinhalten, Weboptionen, Richtlinienlisten für das Neuschreiben von ActiveX-Webinhalten, Richtlinien für das Neuschreiben von ActiveX-Webinhalten, Richtlinienlisten für den Dateizugriff, Richtlinien für den Dateizugriff, Windows- und UNIX-Dateioptionen, Dateiverschlüsselung und Richtlinien für den Webzugriff.

- **Lokale Benutzerkonten** – Benutzer, Authentifizierungsservername, E-Mail-Adresse, vollständiger Name, Anmeldename, Kennwort und Kennwortänderungsoption.

- **Protokoll/Überwachung** – SNMP-Einstellungen, einschließlich Trap-Einstellungen und -Grenzwerte.

HINWEIS: Die obige Liste enthält möglicherweise nicht alle verfügbaren Einstellungen. Eine vollständige Liste der unterstützten Einstellungen finden Sie auf der Seite **XML Import/Export** und der Seite **Push Config** der Webkonsole.

Der grundlegende Prozess für den Export und Import einer XML-Konfigurationsdatei ist wie folgt:

1. Wählen Sie die zu ändernden Konfigurationseinstellungen aus.
2. Exportieren Sie die Datei aus dem IVE.
3. Öffnen Sie die Datei, bearbeiten Sie die Konfigurationsdaten in einem Texteditor.
4. Speichern und schließen Sie die Datei.
5. Importieren Sie die Datei in das IVE.

In den folgenden Abschnitten finden Sie weitere Informationen zu XML-Konfigurationsdateien und ihrer Verwendung:

- „Erstellen und Ändern von XML-Instanzen“ auf Seite 133
- „Strategien für die Arbeit mit XML-Instanzen“ auf Seite 142
- „XML-Konfigurationsdaten exportieren“ auf Seite 366

- „XML-Konfigurationsdaten importieren“ auf Seite 369
- „XML Import/Export – Gebrauchsfälle“ auf Seite 370

Erstellen und Ändern von XML-Instanzen

Wenn Sie Ihre Konfigurationsdatei exportieren, speichert das IVE die Datei als XML-Instanz Die Instanz ist die Datei, die Sie ändern.

Die XML-Instanz

Nach dem Export zeigt Ihnen die Instanzdatei den aktuellen Status der IVE-Konfiguration. Die XML-Instanz basiert auf einem XML-Schema. Das Schema ist eine separate Datei oder eine Gruppe von Dateien, die die Metadaten definieren und als Modell oder Vorlage für die Instanzdatei dienen. Die Schemadatei wird, wenn überhaupt, zu Referenzzwecken verwendet.

Die Daten in der Instanzdatei basieren auf den beim Exportieren auf der Registerkarte **XML Import/Export** der Webkonsole vorgenommenen Einstellungen.

Instanzdateien besitzen normalerweise die Erweiterung *.xml*.

Erstellen einer Instanzdatei

Sie können eine Instanzdatei erstellen, indem Sie eine XML-Konfigurationsdatei aus dem IVE exportieren. Auch wenn Sie alle vorhandenen Konfigurationseinstellungen für ein bestimmtes Objekt ersetzen möchten, sollten Sie mit einer exportierten Instanzdatei beginnen. Die exportierte Instanzdatei enthält alle erforderlichen XML-Verarbeitungsanweisungen und Namespacedeklarationen, deren exakte Definition eingeschlossen werden muss.

Informationen zum Exportieren einer XML-Konfigurationsdatei finden Sie unter „XML-Konfigurationsdaten exportieren“ auf Seite 366.

Bearbeiten der Instanzdatei

Alle XML-Instanzdateien des IVE besitzen eine ähnliche Struktur. Nachdem Sie sich mit der grundlegenden Struktur vertraut gemacht haben, sollten Sie problemlos in den Dateien navigieren können. Da die Dateien groß sein können, ist es mitunter effizienter einen kommerziellen oder Open Source-XML-Editor zu verwenden. XML-Editoren trennen die bearbeitbaren Daten häufig von der Strukturanzeige. Durch diese Trennung wird die Möglichkeit, versehentlich ein XML-Element anstelle seiner Daten zu ändern, weitgehend reduziert. Solche Bearbeitungsfehler sind bei Verwendung eines einfachen Texteditors möglich.

Trotz der potenziellen Vorteile des XML-Editors können Sie Ihre Konfigurationsdaten auch mit einem einfachen Texteditor bearbeiten.

Instanzelemente

Ein Element ist eine separate XML-Einheit, die ein IVE-Objekt oder einen Teil eines Objekts definiert. Das Element besteht normalerweise aus einem Paar von *Tags*, zwischen denen Zeichenfolgendaten stehen können. Tags sind durch spitze Klammern getrennt (< >). In der folgenden Diskussion werden mehrere Beispiele für Tags behandelt.

Jedes Tag kann einem von vier Tagtypen zugeordnet werden:

- **XML-Verarbeitungsanweisung** – Dies ist ein spezieller Tagtyp, der mit einer spitzen Klammer und einem Fragezeichen beginnt (<?) und am Anfang jedes XML-Dokuments zu finden ist. Die XML-Verarbeitungsanweisung darf nicht geändert werden.

- **Start-Tag** – Dieses Tag definiert den Anfang eines Elements. Das Start-Tag besteht aus einer öffnenden spitzen Klammer (<), einem Namen, null oder mehreren Attributen und einer schließenden spitzen Klammer (>). Auf jedes Start-Tag muss ein Ende-Tag im Dokument folgen.

- **Ende-Tag** – Dieses Tag definiert das Ende eines Elements. Das Ende-Tag besteht aus einer öffnenden spitzen Klammer und einem Schrägstrich (</) gefolgt von dem im entsprechenden Start-Tag angegebenen Namen und endet mit einer schließenden spitzen Klammer (>).

- **Leeres Tag** – Das *leere Tag* wird in zwei Formen angegeben. Wenn zwischen einem Tagpaar keine Daten stehen, gilt das Tagpaar als *leeres* Tag. Gemäß der offiziellen XML-Spezifikation sieht ein leeres Tag in etwa wie folgt aus:

  <Beispiel für leeres Tag/>

  In dieser Form besteht das leere Tag aus einer öffnenden spitzen Klammer (<) gefolgt von einem Elementnamen, einem Schrägstrich und einer schließenden spitzen Klammer (/>). Wenn Sie in Ihren Konfigurationsdateien ein leeres Tag sehen, bedeutet dies, dass das jeweilige Element laut Schema in die Instanzdatei eingeschlossen werden muss, seine Daten jedoch optional sind.

Start-Tags können Attribute enthalten und Tagpaare (Elemente) können zusätzliche Elemente enthalten. Das folgende Beispiel zeigt eine XML-Instanzdatei für das Objekt „Users“. In diesem Beispiel werden nur die IVE-Konfigurationseinstellungen für den Plattformadministrator dargestellt. Die fett formatierten Kommentare im Beispiel beschreiben die Tagdetails. Kursiv formatierte Elemente kennzeichnen Benutzerdaten.

```
<!– The file starts with the XML processing instruction. The next two lines are
examples of namespace declarations. You should never delete or modify the
XML processing instruction or namespace declarations. –>

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<IVE xmlns="http://xml.juniper.net/iveos/5.0R1/ive">
<AAA xmlns:aaa="http://xml.juniper.net/iveos/5.0R1/aaa">
    <aaa:Users> <!– Start-Tag –>
        <aaa:User>
            <aaa:AuthServerName>Administrators</aaa:AuthServerName>
            <aaa:Email></aaa:Email> <!– Leeres Tag –>
            <aaa:FullName>IVE Platform Administrator</aaa:FullName>
            <aaa:LoginName>admin</aaa:LoginName>
            <aaa:Password PasswordFormat="Encrypted">fEm3Qs6qBwA
                </aaa:Password> <!– Im Start-Tag definiertes Attribut –>
            <aaa:ChangePasswordAtNextLogin>false
                </aaa:ChangePasswordAtNextLogin>
        </aaa:User>
    </aaa:Users> <!– Ende-Tag –>
```

</AAA> **<!– Ende-Tag für Namespacedeklaration –>**
</IVE> **<!– Ende-Tag für Namespacedeklaration –>**

Sie nehmen Ihre Änderungen an den zwischen den Start- und Ende-Tags angezeigten Zeichenfolgendaten vor. Im obigen Beispiel können Sie z. B. die folgenden Elemente ändern:

- <aaa:AuthServerName>**Administrators**</aaa:AuthServerName>
- <aaa:Email></aaa:Email>
- <aaa:FullName>**IVE Platform Administrator**</aaa:FullName>
- <aaa:LoginName>**admin**</aaa:LoginName>
- <aaa:Password PasswordFormat="Plaintext">**password**</aaa:Password>
- <aaa:ChangePasswordAtNextLogin>**false**</aaa:ChangePasswordAtNextLogin>

HINWEIS: Wenn Sie einen Benutzer für einen bestimmten Authentifizierungsserver oder einen Authentifizierungsserver für einen bestimmten Benutzer ändern, erstellen Sie einen anderen Benutzer – Sie aktualisieren nicht einen vorhandenen Benutzer oder Authentifizierungsserver. Benutzer und Authentifizierungsserver bilden zusammen eine logische Definition eines eindeutigen Benutzers.

Das Element **Email** ist leer. Dies bedeutet, dass das Schema zwar das Element **Email** in der Instanzdatei erfordert, der Wert aber optional ist. Sie können eine E-Mail-Adresse hinzufügen oder das Element leer lassen.

In der Instanzdatei im vorhergehenden Beispiel werden die Daten des Elements **Password** als verschlüsselte Daten dargestellt, und „PasswordFormat“ ist auf „Encrypted“ eingestellt. Dies bedeutet, dass der Kennwortwert nicht geändert werden kann. Der XML-Exportvorgang stellt standardmäßig verschlüsselte Kennwörter bereit, wobei „PasswordFormat“ auf „Encrypted“ eingestellt ist. Sie können das Kennwort ändern, wenn Sie „PasswordFormat“ auf Plaintext setzen. Wenn Sie das Kennwort in der Instanzdatei ändern, ist der Kennwortwert sichtbar, bis er wieder in das IVE importiert wird. Nach dem Import verschlüsselt das IVE das Kennwort.

Wenn Sie Kennwörter für neue Benutzer im Klartextformat eingeben, sind die Kennwörter in der Instanzdatei sichtbar. Die Option **Change Password at Next Login** sollte aus diesem Grund ggf. auf true gesetzt werden.

HINWEIS:

- Da Kennwörter standardmäßig verschlüsselt werden, sind sie vollständig auf andere Systeme übertragbar.
- Versuchen Sie niemals, ein Kennwort manuell in der XML-Datei zu verschlüsseln. Das IVE verweigert alle derartigen Versuche. Verwenden Sie das Klartextkennwortformat (PasswordFormat), und geben Sie beim Ändern von Kennwörtern über die XML-Datei ein Kennwort in Klartext ein.

Attribute

Attribute sind Informationen, die eine Elementdefinition verfeinern. Das Start-Tag eines Elements kann Attribute enthalten. Attributwerte sind durch doppelte Anführungszeichen getrennt. Das folgende Beispiel zeigt das Kennwortelement aus einer Benutzerinstanzdatei. Das Kennwortformat ist als Attribut des Elements definiert:

```
<aaa:Password PasswordFormat="Encrypted">fEm3Qs6qBwBQ</aaa:Password>
```

Sie können den Wert “Encrypted” in einen der anderen zulässigen Werte ändern. Obwohl die zulässigen Werte für ein Attribut häufig in der Webkonsole zu finden sind, müssen Sie für dieses Beispiel die Schemadatei *users.xsd* überprüfen, um die zulässigen Werte Plaintext, Encrypted und Base64 zu identifizieren.

HINWEIS: Die Schemadateien (.xsd) können über die XML-Import-/Exportseiten heruntergeladen werden. Weitere Informationen finden Sie unter „Registerkarte „XML Import/Export““ auf Seite 366.

Namespaces

Namespaces ermöglichen es Ihnen, im Code die gleichen Wörter oder Beschriftungen aus unterschiedlichen Kontexten oder XML-Vokabularien zu verwenden. Wenn Sie Elementen Namespacekennzeichner als Präfix voranstellen, kann eine Instanzdatei Verweise auf unterschiedliche Objekte enthalten, die aus unterschiedlichen XML-Vokabularien stammen und denselben Namen besitzen.

Eine Namespacedeklaration sieht folgendermaßen aus:

```
<AAA xmlns:aaa="http://xml.juniper.net/iveos/5.0R1/aaa">
```

In diesem Beispiel ist der Namespacekennzeichner aaa. Das IVE betrachtet die Elemente <aaa:example> und <xs:example> als gänzlich unterschiedliche Elemente. Sie müssen sich nicht um möglicherweise in Ihren Instanzdateien enthaltene Namespacekennzeichner kümmern, Sie dürfen sie jedoch nicht löschen oder ändern.

Elementreihenfolge

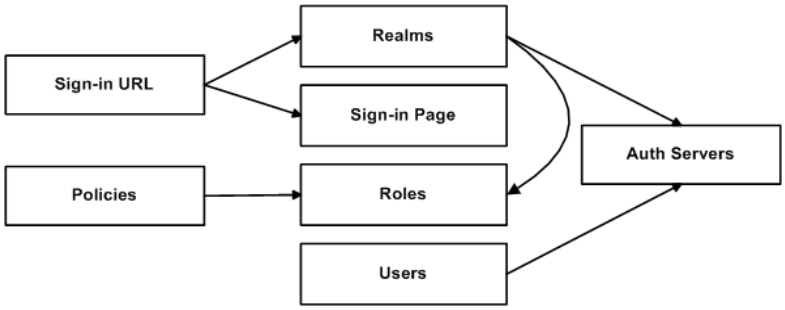
Die Reihenfolge der Elemente in der Instanzdatei sollte möglichst nicht geändert werden. Obwohl das Schema nicht in allen Fällen eine Reihenfolge erzwingt, hat das Ändern der Reihenfolge, in der Elemente in der exportierten Instanzdatei aufgeführt werden, keinerlei Vorteil. In manchen Fällen kann ein Instanzdokument durch das Ändern der Elementreihenfolge ungültig werden.

Einschränkungen der referenziellen Integrität

IVE-Konfigurationsobjekte sind Teil eines Datenmodells, das mithilfe von Einschränkungen der referenziellen Integrität erzwungen wird. Diese Einschränkungen können nicht geändert werden. Sie sollten sich jedoch mit ihnen vertraut machen, bevor Sie Objekte löschen, die Abhängigkeiten von anderen Objekten aufweisen.

Wenn Sie die Einschränkungen der referenziellen Integrität des IVE verletzen, schlägt der Importvorgang fehl. Das folgende Diagramm zeigt die Beziehungen zwischen mehreren IVE-Objekten.

Abbildung 28: Einschränkungen der referenziellen Integrität des IVE



In Abbildung 28 stellen die Felder IVE-Objekttypen dar, und die Pfeile verkörpern Abhängigkeitsbeziehungen zwischen den Objekttypen. Pfeile zeigen vom abhängigen Objekt auf Objekte.

Sie können keine Objekte löschen, von denen ein anderes Objekt abhängig ist. Umgekehrt müssen Sie beim Hinzufügen eines Objekts auch alle anderen Objekte hinzufügen, von denen dieses Objekt abhängig ist.

In Abbildung 28 sind Anmelde-URLs abhängig von Bereichen und Anmeldeseiten. Bereiche sind sowohl von Authentifizierungsservern als auch von Rollen abhängig. Richtlinien sind von Rollen abhängig. Benutzer sind von Authentifizierungsservern abhängig.

Betrachten Sie die folgenden auf Abbildung 28 basierenden Szenarios:

- Wenn Sie Anmelde-URLs hinzufügen, müssen Sie Bereiche, Anmeldeseiten, Rollen und Authentifizierungsserver hinzufügen. Sie müssen einen Authentifizierungsserver und mindestens eine Rolle zur Unterstützung des Bereichs hinzufügen, und der Bereich und die Anmeldeseite müssen zur Unterstützung des neuen Anmelde-URL hinzugefügt werden.

- Wenn Sie einen Benutzer hinzufügen, müssen Sie ihn einem Authentifizierungsserver zuweisen können. Wenn auf dem Ziel-IVE noch kein Authentifizierungsserver eingerichtet ist, müssen Sie in der Instanzdatei einen Server hinzufügen.

- Wenn Sie eine Richtlinie hinzufügen, müssen Sie sie einer Rolle zuweisen können. Wenn auf dem Ziel-IVE noch keine Rolle eingerichtet ist, müssen Sie in der Instanzdatei eine Rolle hinzufügen.

- Wenn Sie einen Authentifizierungsserver löschen, kann dadurch die Funktion von Bereichen und Benutzern beeinträchtigt werden. Daher müssen Sie vor dem Löschen eines Authentifizierungsservers sicherstellen, dass keine Bereiche oder Benutzer von ihm abhängig sind.

- Wenn Sie eine Rolle löschen, können davon Richtlinien und Bereiche betroffen sein. Vor dem Löschen einer Rolle müssen Sie zunächst alle von der Rolle abhängigen Richtlinien löschen oder einer anderen Rolle zuweisen. Darüber hinaus müssen Sie vor dem Löschen einer Rolle alle von dieser Rolle abhängigen Bereiche löschen oder neu zuweisen.

- Durch das Löschen einer Anmeldeseite können Anmelde-URLs fehlschlagen. Vor dem Löschen einer Anmeldeseite müssen Sie zunächst alle zugeordneten Anmelde-URLs löschen oder anderen Anmeldeseiten zuweisen.

Zuordnen der XML-Instanz zu Benutzeroberflächenkomponenten

Die Elemente in der XML-Instanz hängen eng mit den in der Webkonsole angezeigten Objekten und zugehörigen Optionen zusammen. Die Elementnamen in der XML-Instanzdatei entsprechen den angezeigten Objekt- und Optionsnamen.

Öffnen Sie in der Webkonsole z. B. die Seite **Roles > Users > General > Session Options**. Die Webkonsole stellt die möglichen Werte für eine Roamingsitzung als Gruppe von Optionsfeldern mit den folgenden Werten dar:

- Enabled

- Limit to subnet

- Disabled

Der folgende Auszug aus der exportierten Konfigurationsdatei für Rollen zeigt die Sitzungsoptionen für die Rolle „Users“. In der sechsten Zeile (unten fett hervorgehoben) ist die Option für Roamingsitzungen auf Enable gesetzt:

```
<aaa:SessionOptions>
    <aaa:IdleTimeout>10</aaa:IdleTimeout>
    <aaa:MaxTimeout>60</aaa:MaxTimeout>
    <aaa:ReminderTime>5</aaa:ReminderTime>
    <aaa:RoamingNetmask></aaa:RoamingNetmask>
    <aaa:Roaming>Enable</aaa:Roaming>
    <aaa:PersistentPassword>false</aaa:PersistentPassword>
    <aaa:RequestFollowThrough>true</aaa:RequestFollowThrough>
    <aaa:PersistentSession>false</aaa:PersistentSession>
    <aaa:SessionTimeoutWarning>false</aaa:SessionTimeoutWarning>
    <aaa:IgnoreApplicationActivity>false</aaa:IgnoreApplicationActivity>
</aaa:SessionOptions>
```

Sie können die zulässigen Werte für die Option für Roamingsitzungen in der Schemadatei *roles.xsd* ausfindig machen:

```
<xs:simpleType name="EnableRoamingType">
    <xs:restriction base="xs:token">
        <xs:enumeration value="Enable"/>
        <xs:enumeration value="Limited"/>
        <xs:enumeration value="Disable"/>
    </xs:restriction>
</xs:simpleType>
```

Wenn Sie den Wert für die Roamingsitzung von „Enabled“ zu „Limit to subnet“ ändern möchten, ersetzen Sie *Enable* durch *Limited*.

Dieses Beispiel zeigt, dass die Webkonsole häufig alle zulässigen Werte enthält, sei es in Form von Optionsfeldgruppen, Kontrollkästchen, Dropdownlisten oder anderen Benutzeroberflächenkomponenten. Die Instanzdatei zeigt nur den aktuellen Status Ihrer IVE-Konfiguration an. Die Schemadatei zeigt alle von der XML-Import-/Exportfunktion unterstützten tatsächlichen Werte für die Konfigurationsoptionen an.

Weitere Informationen zu spezifischen Elementen können Sie direkt den Schemadateien entnehmen.

XML-Importmodi

Das IVE bietet drei unterschiedliche Importmodi für den Import von XML-Konfigurationsdateien. Die einzelnen Modi ermöglichen stufenweise die Durchführung komplexerer Aufgaben während des Importvorgangs.

Schnellimport

Wenn Sie Ihrer Konfiguration Objekte hinzufügen möchten, verwenden Sie den Schnellimportmodus. Im Schnellimportmodus können keine Änderungen an den vorhandenen Einstellungen vorgenommen werden. Auch wenn Sie die Daten in der XML-Instanzdatei ändern, wendet das IVE diese Änderungen nicht auf die Konfiguration an.

Standardimport

Wenn Sie Objekte ändern oder Ihrer Konfiguration hinzufügen möchten, ohne andere Daten in der Konfiguration zu beeinflussen, verwenden Sie den Standardimportmodus. Im Standardimportmodus können Sie der Konfiguration neue Objekte hinzufügen und vorhandene Objekte aktualisieren. Wenn Sie ein Objekt aus der Instanzdatei löschen und dann den Standardimportmodus verwenden, ignoriert das IVE die Löschung. Das IVE verwendet den Standardimport als standardmäßigen Importmodus.

Vollständiger Import

Der vollständige Importmodus ist der leistungsstärkste Importvorgang, den Sie mit der XML-Instanzdatei ausführen können. Ein vollständiger Import beinhaltet eine vollständige Ersetzung der IVE-Konfiguration. Der vollständige Importmodus ermöglicht das Hinzufügen, Ändern und Löschen von Objekten aus dem IVE.

Da sowohl beabsichtigt als auch unbeabsichtigt erhebliche Änderungen an der Konfiguration vorgenommen werden können, ist es wichtig, dass Sie die Auswirkungen des vollständigen Imports verstehen.

Während eines vollständigen Imports ersetzen Sie Ihre vorhandene Konfiguration komplett durch den Inhalt der Instanzdatei. In diesem Modus können Sie eine große Anzahl von Objekten aus der bestehenden Konfiguration löschen. Das IVE führt die Löschung anhand eines Ausschlussverfahrens durch. Das IVE vergleicht die Instanzdatei mit der vorhandenen Konfiguration und löscht alle Daten, die nicht in der Instanzdatei enthalten sind.

HINWEIS: Bei einer unsachgemäßen Implementierung des vollständigen Imports können Sie versehentlich einen Großteil Ihrer Konfiguration oder sogar die gesamte Konfiguration löschen. Die exportierte Instanzdatei enthält den aktuellen Status der Komponenten der obersten Ebene im IVE.

Die folgenden Szenarios veranschaulichen die falsche und korrekte Verwendung des vollständigen Importmodus bei dem Versuch, einige Benutzer aus einer IVE-Konfiguration zu löschen.

Falsche Verwendung des vollständigen Importmodus

Sie möchten einige Benutzer aus dem IVE entfernen.

HINWEIS: Führen Sie dieses Verfahren NICHT aus. Dieses Verfahren ist ein Beispiel für die falsche Verwendung des vollständigen Importmodus und dient ausschließlich zu Schulungszwecken.

Sie führen folgende Schritte aus:

1. Sie exportieren die lokalen Benutzer, die einem Ihrer Authentifizierungsserver zugeordnet sind.
2. Sie löschen einige der Benutzer aus der XML-Instanzdatei.
3. Sie wählen **Full Import** aus und importieren die verbleibenden Benutzer wieder in das IVE.

Sie haben nun alle Benutzer gelöscht *außer* denjenigen, die in der XML-Instanzdatei übrig geblieben sind. Ihr Fehler bestand darin, dass Sie nur die mit einem spezifischen Authentifizierungsserver verknüpften Benutzer exportiert haben. Da der vollständige Importmodus eine vollständige Ersetzung der Konfiguration zur Folge hat, überschreibt der Inhalt der importierten Datei alle entsprechenden IVE-Konfigurationsdaten.

Korrekte Verwendung des vollständigen Importmodus

Sie möchten einige Benutzer aus dem IVE entfernen. Sie führen folgende Schritte aus:

1. Sie exportieren **alle** lokalen Benutzer aus **allen** im IVE definierten Authentifizierungsservern.

2. Sie löschen einige der Benutzer aus der XML-Instanzdatei.

3. Sie wählen **Full Import** aus und importieren die verbleibenden Benutzer wieder in das IVE.

Sie haben jetzt nur die ausgewählten Benutzer aus dem IVE gelöscht, und die anderen Benutzer sind intakt geblieben.

Überprüfen der Instanzdatei

Ein XML-Schema definiert die Struktur einer Anwendung sowie zulässige Werte, Standardwerte, Datentypen, Bereiche, Listenwerte, erforderliche und optionale Werte, die Syntax und andere Datenstrukturen. Die XML-Instanz wird mit dem Schema verglichen, wenn Sie versuchen, die Instanz in das IVE zu importieren. Dadurch wird sichergestellt, dass die Instanz den Anforderungen für eine gültige IVE-Konfiguration entspricht.

Wenn Sie Änderungen an der Instanzdatei vorgenommen haben, die gegen die im Schema definierten Regeln verstoßen – z. B. Regeln zur referenziellen Integrität, zu zulässigen Werten, Bereichen oder anderen Einschränkungstypen –, führt das IVE den Importvorgang nicht aus, und es werden Fehlermeldungen angezeigt.

Sie können die Schemadateien (.xsd) für die IVE-Objekte herunterladen, deren Daten für den Export und Import verfügbar sind. Die Schemadateien können beim Festlegen der Regeln für die IVE-Objekte hilfreich sein, da sie sich auf das Exportieren, Ändern und Importieren dieser Objekte beziehen.

Herunterladen von Schemadateien

Sie können die Schemadateien (.xsd) für die IVE-Objekte herunterladen, wenn Sie die für die Objekte geltenden Strukturen und Regeln überprüfen möchten.

Die Schemadaeien sind nach Objekttyp in separaten Dateien organisiert. Das Schema für lokale Benutzerkonten finden Sie z. B. in der Datei „users.xsd“. Die Dateien sind alle in einer ZIP-Datei enthalten.

Zum Herunterladen der ZIP-Datei stehen zwei Methoden zur Auswahl:

- Über die XML-Import-/Exportseiten durch Klicken auf einen Hyperlink
- Durch direkten Zugriff auf den URL, unter dem die Dateien im System gespeichert sind

Weitere Informationen zum Herunterladen von Schemadateien über die XML-Import-/Exportseiten finden Sie unter „Registerkarte „XML Import/Export““ auf Seite 366.

Rufen Sie für den Zugriff auf die ZIP-Datei mit den XSD-Dateien den folgenden URL direkt oder über ein Skript auf:

https://<IVE-IP-oder-Hostname>/dana-na/xml/schema.zip

Dabei ist IVE-IP-oder-Hostname die IP-Adresse bzw. der Hostname des IVE. Bei dieser Methode müssen Sie sich nicht am IVE anmelden.

HINWEIS: Diese Funktion wird in der Zukunft möglicherweise geändert. Bedenken Sie dies, wenn Sie mithilfe von Skripts über den URL auf die ZIP-Datei zugreifen. Folgende Elemente können sich ändern:

- Der URL.
- Der Dateiname.
- Die Dateierweiterung. Das Format kann sich z. B. zu XSD ändern.
- Die Anzahl von Dateien. Anstelle der Verwendung einzelner objektspezifischer Schemadateien können die Dateien in einer vollständigen XSD-Datei kombiniert werden.

Strategien für die Arbeit mit XML-Instanzen

Die folgenden Strategien können beim Exportieren und Importieren von XML-Instanzdateien hilfreich sein:

- Definieren Sie Ihr Ziel für einen **XML Import/Export**-Vorgang.
  - Welche IVE-Objekte müssen hinzugefügt, aktualisiert oder gelöscht werden?
  - Müssen alle Änderungen in einem Arbeitsschritt durchgeführt werden, oder können Sie die Konfiguration in separaten Arbeitsschritten ändern?
  - Ist der Prozess ein einmaliger Vorgang, oder müssen Sie den gleichen Vorgang mehrmals ausführen?
  - Aktualisieren Sie ein vorhandenes IVE, oder verwenden Sie eine IVE-Konfiguration als Vorlage zum Konfigurieren anderer IVEs?
- Dokumentieren Sie die Änderungen, die an den IVE-Objekten vorgenommen werden sollen.
  - Erstellen Sie eine Liste der Objekte, die hinzugefügt, aktualisiert oder gelöscht werden sollen.
  - Listen Sie für die hinzuzufügenden oder zu aktualisierenden Objekte spezifische Attributdaten auf.
  - Listen Sie Seiten oder Registerkarten aus der Webkonsole auf, die den zu ändernden Objekten und Attributen entsprechen.
- Erstellen Sie unmittelbar vor der Durchführung des Imports einen binären Systemsnapshot oder eine binäre Konfigurationssicherung.
- Prüfen Sie nochmals die unter „XML-Importmodi“ auf Seite 139 beschriebenen Auswirkungen der Importmodi.
- Erstellen Sie einen Plan, anhand dessen Sie überprüfen, ob die erstellte Konfiguration Ihren Anforderungen entspricht.

- Überprüfen Sie im Administratorprotokoll (Admin Access Log), ob die Export- und Importvorgänge erfolgreich ausgeführt wurden.

- Führen Sie eine Stichprobe der geänderten Objekte aus. Vergewissern Sie sich, dass die Objekte wie erwartet hinzugefügt, aktualisiert oder gelöscht wurden.

In nahezu allen Fällen müssen Sie sowohl die XML-Instanzdatei als auch die Webkonsole verwenden. Dies gilt insbesondere, wenn Sie erstmals XML-Instanzdateien ändern. Darüber hinaus müssen Sie möglicherweise die XML-Schemadateien zu Rate ziehen.

Verwenden Sie die XML-Instanzdatei für folgende Aufgaben:

- Identifizieren der als XML-Elemente dargestellten Konfigurationsobjekte

- Suchen und Ändern der Konfigurationsdaten

Verwenden Sie die Webkonsole für folgende Aufgaben:

- Zuordnen visueller Komponenten zu XML-Schemaelementen und -Instanzelementen

- Bestätigen der Genauigkeit von Änderungen an bestimmten Objekten

Verwenden Sie die XML-Schemadatei für folgende Aufgaben:

- Identifizieren der Struktur und Reihenfolge von Konfigurationsobjekten

- Identifizieren von optionalen und erforderlichen Elementen, zulässigen Werten, Standardwerten und anderen Attributen der Konfigurationsobjekte Weitere Informationen finden Sie unter „Registerkarte „XML Import/Export““ auf Seite 366.

Aufgabenzusammenfassung: Importieren und Exportieren von XML-Konfigurationsdateien

1. XML-Konfigurationsdateien können über die Seite **Maintenance > Import/Export > Export** der Webkonsole exportiert werden. Anweisungen hierfür finden Sie unter „XML-Konfigurationsdaten exportieren“ auf Seite 366.

2. XML-Konfigurationsdateien können über die Seite **Maintenance > Import/Export > Import** der Webkonsole importiert werden. Anweisungen hierfür finden Sie unter „XML-Konfigurationsdaten importieren“ auf Seite 369.

Fehlerbehebung – Übersicht

Dieser Abschnitt bietet einen Überblick über die verschiedenen über das IVE verfügbaren Fehlerbehebungsaufgaben:

- „Simulieren oder Verfolgen von Ereignissen“ auf Seite 144
- „Erstellen von Snapshots des IVE-Systemstatus“ auf Seite 145
- „Erstellen von TCP-Dumpdateien“ auf Seite 145
- „Testen der IVE-Netzwerkverbindung“ auf Seite 146
- „Remoteausführung von Debuggingtools“ auf Seite 147
- „Erstellen von Debuggingprotokollen“ auf Seite 147

Simulieren oder Verfolgen von Ereignissen

Sie können feststellen, weshalb das IVE Ihnen die Ausführung einer bestimmten Aufgabe nicht erlaubt, indem Sie problematische IVE-Ereignisse mit den Einstellungen auf der Seite **Maintenance > Troubleshooting > User Sessions** der Webkonsole simulieren und verfolgen. Diese Seite enthält alle zurzeit im IVE konfigurierten Bereiche, Rollen und Richtlinien sowie Protokollmeldungen aus unterschiedlichen Phasen des Authentifizierungs-, Autorisierungs- und Zugriffsprozesses.

Die relevanten Ereignissen beziehen sich auf die Authentifizierung, die Autorisierung und den Zugriff für einen bestimmten Benutzer. Sie hängen gänzlich von den Geschehnissen während einer Benutzersitzung ab. Dies gilt sowohl für die Simulation als auch die Richtlinienverfolgung.

HINWEIS: Die erfassten Ereignisse enthalten keine anderen systemspezifischen Ereignisse. Das IVE verwendet die Ereignisse bloß als Filtermechanismus, um die Anzahl von Protokollen zu reduzieren und das Problem hervorzuheben.

Simulieren von problemverursachenden Ereignissen

Das IVE ermöglicht die Behebung von Problemen durch Simulation der Ereignisse, die das Problem verursachen. Auf der Seite **Maintenance > Troubleshooting > User Sessions > Simulation** können Sie virtuelle Benutzersitzungen erstellen, ohne dass sich die Endbenutzer am IVE anmelden und die entsprechenden Probleme reproduzieren müssen. Zudem können Sie die Registerkarte **Simulation** verwenden, um neue Authentifizierungs- und Autorisierungsrichtlinien vor der Verwendung in einer Produktionsumgebung zu testen.

Zur Verwendung der Simulation müssen Sie die zu simulierenden Ereignisse angeben. (Sie können z. B. eine virtuelle Sitzung erstellen, in der sich „John Doe“ um 6:00 Uhr über einen Internet Explorer-Browser am Bereich „Users“ anmeldet.) Anschließend müssen Sie angeben, welche Ereignisse in der Simulation aufgezeichnet und protokolliert werden sollen. Sie können im Simulationsprotokoll drei Haupttypen von Ereignissen aufzeichnen:

- **Vor der Authentifizierung** – Die erfassten IVE-Ereignisse enthalten keine anderen systemspezifischen Ereignisse. Ereignisse werden nur als Filtermechanismus verwendet, um die Anzahl von Protokollen zu reduzieren und das Problem hervorzuheben.

- **Rollenzuordnung** – Die erfassten IVE-Ereignisse enthalten keine anderen systemspezifischen Ereignisse. Ereignisse werden nur als Filtermechanismus verwendet, um die Anzahl von Protokollen zu reduzieren und das Problem hervorzuheben.

- **Ressourcenrichtlinien** – Die erfassten IVE-Ereignisse enthalten keine anderen systemspezifischen Ereignisse. Ereignisse werden nur als Filtermechanismus verwendet, um die Anzahl von Protokollen zu reduzieren und das Problem hervorzuheben.

Verfolgen von Ereignissen mithilfe der Richtlinienverfolgung

Das IVE ermöglicht die Behebung von Problemen, indem Sie die Ereignisse bei der Anmeldung eines Benutzers an einem Bereich verfolgen. Auf der Seite **Maintenance > Troubleshooting > User Sessions > Policy Tracing** können Sie eine Richtlinienverfolgungsdatei für einen Benutzer aufzeichnen. Das IVE zeigt Protokolleinträge mit den Aktionen des Benutzers mit einem Hinweis an, weshalb dem Benutzer der Zugriff auf verschiedene Funktionen wie das Web oder einen Dateiserver gewährt oder verweigert wird.

Erstellen von Snapshots des IVE-Systemstatus

Auf der Registerkarte **Maintenance > Troubleshooting > System Snapshot** kann ein Snapshot des IVE-Systemstatus erstellt werden. Wenn Sie diese Option verwenden, führt das IVE verschiedene Dienstprogramme aus, um Details zum IVE-Systemstatus zu erfassen, z. B. zum belegten Speicherplatz, zur Auslagerungsleistung, zur Anzahl der ausgeführten Prozesse, zur Systembetriebszeit, zur Anzahl der geöffneten Dateibeschreibungen und zu den verwendeten Ports. Das IVE speichert bis zu zehn Snapshots, die in einer verschlüsselten „Dumpdatei“ bzw. Sicherungsdatei abgelegt werden. Diese können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den Juniper Networks-Support senden.

Erstellen von TCP-Dumpdateien

Auf der Registerkarte **Maintenance > Troubleshooting > TCP Dump** können Sie Netzwerkpaketheader sniffen und die Ergebnisse in einer verschlüsselten „Dumpdatei“ speichern. Diese Datei können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den Juniper Networks-Support senden.

Diese Funktion verwendet den TCP/IP-Netzwerkstack, um Pakete auf der TCP-Ebene zu erfassen. Sie erfasst die gesamte Kommunikation durch das IVE. Bestimmte verschlüsselte komplexere Protokolle können jedoch nicht entschlüsselt werden. Diese Funktion eignet sich für die Behebung von allgemeinen Kundenproblemen. Eine TCP-Dumpdatei hilft dem Juniper Networks-Supportteam, die zwischen dem IVE und einem anderen Intranetserver verwendeten Kommunikationsprotokolle und die Reaktion des Intranetservers auf Anfragen vom IVE zu beobachten.

Auf der Webkonsole können Sie die Schnittstelle auswählen, von der Pakete erfasst werden sollen (intern oder extern), Sie können den Promiscuous-Modus aktivieren, um die Detailstufe der Dumpdatei zu erhöhen, und Sie können einen Filter festlegen.

Testen der IVE-Netzwerkverbindung

Auf der Registerkarte **Maintenance > Troubleshooting > Commands** können Sie UNIX-Befehle wie arp, ping, traceroute und NSlookup ausführen, um die IVE-Netzwerkverbindung zu testen. Mit diesen Verbindungstools können Sie den Netzwerkpfad vom IVE zu einem bestimmten Server anzeigen. Sie können einen ping- oder traceroute-Befehl an das IVE senden, und das IVE kann den ping-Befehl für den Zielserver ausführen. Remotebenutzer sollten in der Lage sein, über das IVE auf den Server zuzugreifen.

Address Resolution Protocol (ARP)

Verwenden Sie den arp-Befehl, um IP-Netzwerkadressen Hardwareadressen zuzuordnen. Das Address Resolution Protocol (ARP) ermöglicht die Auflösung von Hardwareadressen.

Um die Adresse eines Servers im Netzwerk aufzulösen, sendet ein Clientprozess auf dem IVE Informationen über dessen eindeutige Identität an einen auf einem Server im Intranet ausgeführten Serverprozess. Der Serverprozess gibt dann die erforderliche Adresse an den Clientprozess zurück.

Ping

Mit dem ping-Befehl können Sie überprüfen, ob das IVE eine Verbindung mit anderen Systemen im Netzwerk herstellen kann. Im Fall eines Netzwerkfehlers zwischen den lokalen Knoten und Remoteknoten erhalten Sie keine Antwort von einem gepingten Gerät. Bitten Sie in diesem Fall Ihren LAN-Administrator um Hilfe.

Der ping-Befehl sendet Pakete an einen Server und gibt die Antwort des Servers zurück. Hierbei handelt es sich normalerweise um einen Satz von Statistiken mit der IP-Adresse des Zielservers, der zum Senden von Paketen und Empfangen der Antwort erforderlichen Zeit und anderen Daten. Der ping-Befehl kann für Unicast- oder Multicastadressen ausgeführt werden, und der Name des Zielservers muss in der Anfrage enthalten sein.

Traceroute

Mit dem traceroute-Befehl können Sie den Pfad ermitteln, über den ein Paket vom IVE zu einem anderen Host gesendet wird. Traceroute sendet ein Paket an einen Zielserver und empfängt eine ICMP TIME_EXCEEDED-Antwort von jedem Gateway auf dem Pfad. Die TIME_EXCEEDED-Antworten und andere Daten werden aufgezeichnet und in der Ausgabe mit dem Pfad des Round-Trips angezeigt.

NSlookup

Mit dem Nslookup-Befehl können Sie detaillierte Informationen zu einem Namenserver im Netzwerk abrufen. Sie können mehrere unterschiedliche Informationstypen abfragen, z. B. IP-Adresse eines Servers, Alias-IP-Adresse, Autoritätsursprungseintrag, Exchange-Maileintrag, Benutzerinformationen, WKS-Informationen (Well-Known Services) usw.

Remoteausführung von Debuggingtools

Das Team des Juniper Networks-Support kann Debuggingtools in Ihrem Produktions-IVE ausführen, wenn Sie es über die Seite **Maintenance > Troubleshooting > Remote Debugging** entsprechend konfigurieren. Zur Aktivierung dieser Option müssen Sie mit dem Juniper Networks-Support zusammenarbeiten, um einen Debuggingcode sowie einen Host zu erhalten, mit dem das IVE eine Verbindung herstellt.

Erstellen von Debuggingprotokollen

Wenn Sie ein Problem haben, bittet der Mitarbeiter des Juniper Networks-Support Sie möglicherweise, Debuggingprotokolle für die Behebung von internen IVE-Problemen zu erstellen. Wenn die Protokollierung aktiviert ist, zeichnet das IVE entsprechend den auf der Registerkarte **Maintenance > Troubleshooting > Debug Log** der Webkonsole eingegebenen Ereigniscodes bestimmte Ereignisse und Meldungen auf. Anhand des resultieren Debugprotokolls kann das Supportteam dann den Codeverlauf überprüfen und Abweichungen feststellen. Die erforderlichen Informationen zum Erstellen der Protokolldatei (einschließlich der Debugdetailstufe und Ereigniscodes) erhalten Sie vom Supportmitarbeiter.

Unterstützung mehrerer Sprachen – Übersicht

SSL-VPN-Appliances unterstützen die Dateicodierung, die Anzeige der Endbenutzeroberfläche und angepasste Anmelde- und Systemseiten in mehreren Sprachen. SSL-VPN-Appliances unterstützen die folgenden Sprachen:

- Englisch (US)
- Chinesisch (VR China)
- Chinesisch (Taiwan)
- Französisch
- Deutsch
- Japanisch
- Korean
- Spanisch

Das IVE ermöglicht die Anzeige der Endbenutzeroberfläche in einer der unterstützten Sprachen. Diese Funktion ermöglicht in Verbindung mit angepassten Anmelde- und Systemseiten und einem lokalisierten Betriebssystem das Arbeiten in einer vollständig lokalisierten Umgebung.

Beim Festlegen einer Sprache zeigt das IVE die Benutzeroberfläche einschließlich aller Menüs, der vom IVE erstellten Dialogfelder und der Hilfedatei in der ausgewählten Sprache an, unabhängig davon, an welchem Bereich sich die Benutzer anmelden. Verwenden Sie zum Konfigurieren von Lokalisierungsoptionen die Einstellungen auf der Registerkarte **Maintenance > System > Options**. Anweisungen hierfür finden Sie unter „Registerkarte „Options““ auf Seite 361.

Teil 3

IVE Konfiguration

Dieser Abschnitt enthält IVE-Anweisungen für die Konfiguration und Wartung des IVE über die Webkonsole. Der Aufbau des Abschnitts entspricht der Struktur der Webkonsole, so dass Sie die Anweisungen für eine bestimmte Seite in der Benutzeroberfläche leicht finden können.

Inhalt

- „Systemeinstellungen“ auf Seite 153
- „Administratoreinstellungen“ auf Seite 255
- „Benutzereinstellungen“ auf Seite 273
- „Ressourcenrichtlinieneinstellungen“ auf Seite 303
- „Wartungseinstellungen“ auf Seite 357

Aufgabenzusammenfassungen

Inhalt

Aufgabenzusammenfassung: Konfigurieren von Produkten auf Basis der IVE-Plattform 35
Aufgabenzusammenfassung: Konfigurieren von Anmelderichtlinien 55
Aufgabenzusammenfassung: Konfiguration des IVE zum Signieren oder Neusignieren von Java-Applets 73
Aufgabenzusammenfassung: Konfigurieren von Host Checker 86
Aufgabenzusammenfassung: Konfigurieren von Network Connect 104
Aufgabenzusammenfassung: Konfigurieren eines E-Mail-Clients im IVE 110
Aufgabenzusammenfassung: Hochladen und Aktivieren von Java-Applets 115
Aufgabenzusammenfassung: Konfigurieren eines Durchgangsproxy 119
Aufgabenzusammenfassung: Importieren und Exportieren von Konfigurationsdateien und Benutzerkonten 130
Aufgabenzusammenfassung: Importieren und Exportieren von XML-Konfigurationsdateien 143

Kapitel 6

Systemeinstellungen

Mit den Einstellungen im Abschnitt **System** der Webkonsole können Sie die IVE- und Benutzeraktivität überwachen, allgemeine System- und Netzwerkeinstellungen konfigurieren und Systemprotokolle anzeigen.

Inhalt

- „Konfigurieren der Seite „Status““ auf Seite 155
- „Konfigurieren der Seite „Configuration““ auf Seite 158
- „Konfigurieren der Seite „Network““ auf Seite 186
- „Konfigurieren der Seite „Log Monitoring““ auf Seite 191

Konfigurieren der Seite „Status“

Die Seite **Status** enthält die folgenden Registerkarten:

- „Registerkarte „Overview““ auf Seite 155 – Diese Registerkarte dient zum Herunterladen des aktuellen Dienstpakets und Bearbeiten des Datums und der Uhrzeit des Systems.
- „Registerkarte „Active Users““ auf Seite 156 – Diese Registerkarte dient zum Überwachen der am IVE angemeldeten Benutzer.

Registerkarte „Overview“

Wenn Sie sich an der Webkonsole anmelden, ist die Seite **System > Status** ausgewählt, und die Registerkarte **Overview** wird angezeigt. Auf dieser Registerkarte sind die Details zum IVE-Server und den Systembenutzern zusammengefasst. Wenn Sie auf anderen Seiten der Webkonsole Änderungen vornehmen, werden die entsprechenden Informationen auf der Seite **Overview** aktualisiert.

Herunterladen des aktuellen Dienstpakets

Auf der Registerkarte **System > Status > Overview** können Sie das Dienstpaket herunterladen, dass zurzeit im IVE installiert ist, damit Sie es leicht speichern und auf einem anderen IVE installieren können.

So laden Sie das aktuelle Dienstpaket herunter:

1. Wählen Sie in der Webkonsole die Optionen **System > Status > Overview** aus.
2. Klicken Sie auf die Verknüpfung neben **System Software Pkg Version**.
3. Klicken Sie auf **Save**.
4. Geben Sie einen Namen und einen Speicherort für das Dienstpaket an.
5. Klicken Sie auf **Save**.

Bearbeiten von Systemdatum und -zeit

Sie müssen die Serverzeit einstellen, damit die Systemereignisse und die Übertragung von Benutzerdateien genau aufgezeichnet werden. Sie können das IVE über einen NTP-Server (Network Time Protocol) mit anderen Computern synchronisieren oder die IVE-Zeit manuell einrichten.

So bearbeiten Sie Systemdatum und -zeit:

1. Wählen Sie in der Webkonsole die Optionen **System > Status > Overview** aus.
2. Klicken Sie im Abschnitt **System Date & Time** auf **Edit**.

3. Wählen Sie im Menü **Time Zone** eine Zeitzone aus. Das IVE passt die Uhrzeit automatisch an die Sommerzeit an.

4. Stellen Sie die Systemzeit mithilfe einer der folgenden Methoden ein:

   - **Use NTP server** – Wählen Sie die Option **Use NTP Server** aus, geben Sie die IP-Adresse oder den Namen des Servers ein, und geben Sie ein Aktualisierungsintervall an.

   - **Set Time Manually** – Wählen Sie die Option **Set Time Manually** aus, und geben Sie Werte für Datum und Uhrzeit ein. Sie können auch auf **Get from Browser** klicken, damit Daten in die Felder **Date** und **Time** eingegeben werden.

5. Klicken Sie auf **Save Changes**.

Registerkarte „Active Users“

Über das Menü **Active Users** können Sie Benutzer überwachen, die am IVE angemeldet sind. Dabei werden der Name jedes Benutzers, der Authentifizierungsbereich und die Anmeldezeit aufgeführt.

So überwachen Sie am IVE angemeldete Benutzer:

1. Wählen Sie in der Webkonsole die Optionen **System > Status > Active Users** aus.

2. Führen Sie bei Bedarf die folgenden Vorgänge durch:

   - **Abmelden von Benutzern von einer IVE-Sitzung:**

     - Um einen oder mehrere Endbenutzer oder Administratoren zwangsweise abzumelden, aktiveren Sie die Kontrollkästchen neben den entsprechenden Namen, und klicken Sie dann auf **Delete Session**.

     - Um alle aktuell angemeldeten Endbenutzer zwangsweise abzumelden, klicken Sie auf **Delete All Sessions**.

HINWEIS: Zum Abmelden von Administratoren müssen Sie diese einzeln auswählen und auf die Schaltfläche **Delete Session** klicken.

- **Durchführen einer dynamischen Richtlinienauswertung aller angemeldeten Benutzer:**

  - Klicken Sie auf **Refresh Roles**, um alle Authentifizierungsrichtlinien, Rollenzuordnungsregeln, Rolleneinschränkungen und Ressourcenrichtlinien für alle derzeit angemeldeten Benutzer manuell auszuwerten. Verwenden Sie diese Schaltfläche, wenn Sie Änderungen an einer Authentifizierungsrichtlinie, an Rollenzuordnungsregeln, Rolleneinschränkungen oder Ressourcenrichtlinien vornehmen möchten, und die Rollen aller Benutzer sofort aktualisiert werden sollen. Weitere Informationen finden Sie unter „Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)“ auf Seite 44.

- **Konfigurieren der angezeigten Daten und ihrer Reihenfolge:**

  - Geben Sie zum Anzeigen eines bestimmten Benutzers seinen Benutzernamen im Feld **Show Users Named** ein, und klicken Sie auf **Update**. Wenn Sie den genauen Benutzernamen nicht kennen, verwenden Sie einen Platzhalter (*). Wenn z. B. ein Benutzer „Joseph Jones“ heißt, Sie sich aber nicht erinnern können, ob der Benutzername „Joe“ oder „Joseph“ lautet, geben Sie im Feld **Show Users Named** die Zeichenfolge „Jo*“ ein Das IVE gibt eine Liste aller Benutzer zurück, deren Benutzername mit den Buchstaben „jo“ beginnt.

  - Um festzulegen, wie viele Benutzer und Administratoren auf der Seite **Active Users** angezeigt werden, geben Sie eine Zahl ins Feld **Show N users** ein, und klicken Sie auf **Update**.

  - Um die Tabelle der aktuell angemeldeten Benutzer und Administratoren zu sortieren, klicken Sie auf eine Spaltenüberschrift.

  - Klicken Sie zum Aktualisieren des Seiteninhalts auf **Update**.

- **Erstellen einer Verknüpfung mit weiteren Registerkarten:**

  - Klicken Sie zum Bearbeiten des Authentifizierungsbereichs eines Benutzers neben dem Namen auf die Verknüpfung **Realm**, und folgen Sie den Anweisungen unter „Erstellen eines Authentifizierungsbereichs“ auf Seite 257.

  - Klicken Sie zum Bearbeiten der Rolle eines Benutzers auf die Verknüpfung **Role** neben seinem Namen, und folgen Sie den Anweisungen unter „Konfigurieren der Seite „Delegation““ auf Seite 267 (für Administratoren) oder „Konfigurieren der Seite „Roles““ auf Seite 276 (für Endbenutzer).

Konfigurieren der Seite „Configuration“

Die Seite **Configuration** enthält die folgenden Registerkarten:

- „Registerkarte „Licensing““ auf Seite 158 – Diese Registerkarte dient zum Eingeben oder Aktualisieren der IVE-Lizenzen.
- „Seite „Security““ auf Seite 164 – Diese Seite dient zum Festlegen der Standardsicherheitseinstellungen.
- „Registerkarten „Certificates““ auf Seite 166 – Diese Registerkarten dienen zum Hochladen von Server-, Client- und Codesignaturzertifikaten in das IVE, Herunterladen von Zertifikaten vom IVE, Erneuern von Zertifikaten, Löschen von Zertifikaten, Erstellen von Zertifikatssignaturanforderungen (CSR) für neue Zertifikate, Importieren von signierten Zertifikaten aus einer CSR, Aktivieren der CRL-Prüfung und Anzeigen von Zertifikatdetails.
- „Registerkarte „NCP““ auf Seite 182 – Diese Registerkarte dient zum Einrichten von NCP-Optionen für Windows- und Java-Clients.

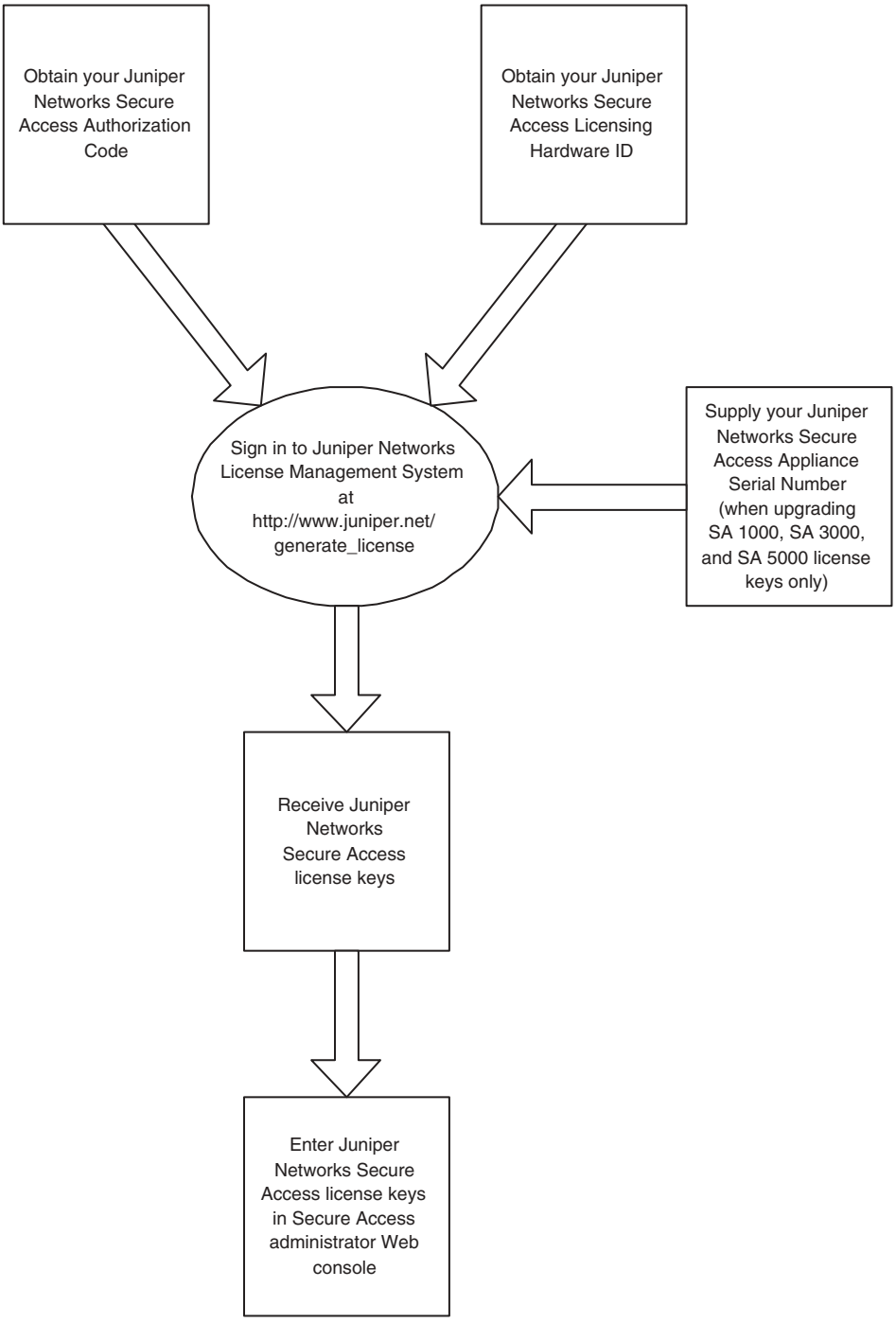
Registerkarte „Licensing“

Die Secure Access 700-Appliance enthält eine Lizenz für den Standardzugriff auf das IVE. Um die Appliance im vollen Umfang nutzen zu können, müssen Sie jedoch auf das Juniper Networks-Lizenzverwaltungssystem zugreifen. Dort geben Sie Ihre Lizenzierungshardware-ID und Autorisierungscodes ein, um die Lizenzschlüssel abzurufen, und anschließend melden Sie sich an der Administrator-Webkonsole an, um die von Juniper Networks bereitgestellten Lizenzschlüssel einzugeben.

Eine *Lizenzierungshardware-ID* ist ein eindeutiger, aus 16 Zeichen bestehender Code, anhand dessen Juniper Networks Ihr spezielles IVE beim Generieren von Lizenzschlüsseln identifiziert. Die Lizenzierungshardware-ID des IVE wird über den Menüoptionen in der seriellen Konsole und unten in der Administrator-Webkonsole angezeigt.

Ein *Autorisierungscode* ist ein Hauptschlüssel, der zum Generieren und Aktivieren der für das IVE erworbenen Secure Access-Lizenzschlüssel erforderlich ist. Sie erhalten Ihre *Autorisierungscodes* getrennt vom IVE, nachdem Sie das IVE und die zugehörigen Produkt- und Funktionslizenzen erworben haben.

Abbildung 29: Generierung und Aktivierung von Lizenzschlüsseln


Obtain your Juniper Networks Secure Access Authorization Code
Obtain your Juniper Networks Secure Access Licensing Hardware ID
Sign in to Juniper Networks License Management System at http://www.juniper.net/generate_license
Supply your Juniper Networks Secure Access Appliance Serial Number (when upgrading SA 1000, SA 3000, and SA 5000 license keys only)
Receive Juniper Networks Secure Access license keys
Enter Juniper Networks Secure Access license keys in Secure Access administrator Web console

Das vom Juniper Networks-Lizenzverwaltungssystem heruntergeladene Paket bzw. die E-Mail, die Sie von Juniper Networks erhalten, können unterschiedliche Lizenztypen enthalten:

- **Seure Access 700-Standardzugriffslizenzschlüssel** – Die Secure Access 700-Standardzugriffslizenzschlüssel unterstützen 10, 15 oder 25 Benutzer und bieten über Network Connect Zugriff auf das IVE. Zusätzlich können Sie Lizenzschlüssel für den Zugriff auf Network Connect und Kernzugriffsmethoden wie Terminaldienste und Weblesezeichen erwerben. SA 700-Standardlizenzschlüssel sind *additiv*, d. h., Sie können die Anzahl von Benutzern, die auf das IVE zugreifen können, einfach erweitern, indem Sie einen weiteren Lizenzschlüssel erwerben und der Konfiguration hinzufügen. Wenn Sie zunächst z. B. eine SA700-ADD-10U-Lizenz erwerben und dann später eine weitere SA700-ADD-10U-Lizenz erwerben, können bis zu 20 Benutzer auf Ihr IVE zugreifen.

- **SA 700-Kernzugriffs-Aktualisierungslizenzschlüssel** – Secure Access 700-Kernzugriffs-Aktualisierungslizenzschlüssel sind eine Aktualisierungsoption für Remote Access 500-Kunden. Sie ermöglichen die Nutzung von Kernzugriffsfunktionen wie Terminaldienste und Weblesezeichen, ohne neue Secure Access 700-Zugriffslizenzschlüssel erwerben zu müssen.

Geben Sie auf der Registerkarte **System > Configuration > Licensing** die Lizenzschlüssel für Ihre Site ein, zeigen Sie die Ablaufdaten ein, und löschen Sie diese ggf.

HINWEIS: Lesen Sie in jedem Fall die Lizenzvereinbarung, auf die Sie über die Registerkarte **Licensing** zugreifen können, bevor Sie Ihren Lizenzschlüssel senden. Bei der über die Registerkarte **Licensing** verfügbaren Lizenzvereinbarung handelt es sich um denselben Text, der während des ersten Setups an der seriellen Konsole angezeigt wird.

Erstellen neuer IVE-Lizenzschlüssel oder Übertragen von Lizenzschlüssel auf ein Ersatz-IVE

So erstellen Sie neue IVE-Lizenzschlüssel und geben Sie diese ein oder übertragen Sie Lizenzschlüsssel auf ein Ersatz-IVE:

1. Vergewissern Sie sich, dass Sie Ihre Lizenzierungshardware-ID und Autorisierungscodes zur Hand haben.

   Die *Lizenzierungshardware-ID* des IVE wird über den Menüoptionen in der seriellen Konsole und unten in der Administrator-Webkonsole angezeigt.

   Sie erhalten Ihre *Autorisierungscodes* getrennt vom IVE, nachdem Sie das IVE und die zugehörigen Produkt- und Funktionslizenzen erworben haben.

2. Navigieren Sie zum Juniper Networks-Lizenzverwaltungssystem unter https://www.juniper.net/generate_license.

HINWEIS: Das Juniper Networks-Lizenzverwaltungssystem enthält einen Zugriffspunkt, über den Sie detaillierte Informationen zu Juniper Networks-Lizenzen abrufen können. Dies beinhaltet auch alle für Sie und Ihre Firma registrierten Lizenzen und alle Lizenzen, die derzeit spezifischen Lizenzierungshardware-IDs zugeordnet sind.

Sie benötigen eine gültige Benutzer-ID und ein gültiges Kennwort für das Juniper Networks Customer Support Center, um an dieser Stelle auf die Informationen zuzugreifen. Anmeldeinformationen für das Juniper Networks Customer Support Center erhalten Sie über die Customer Support Center-Website unter https://www.juniper.net/customers/support/.

---

3. Klicken Sie auf den Link **Secure Access SSL VPN**, um neue IVE-Lizenzschlüssel zu generieren, oder klicken Sie auf **Generate Replacement License for RMA Device**, um basierend auf einer vorhandenen Lizenz einen Lizenzschlüssel für ein IVE zu erstellen, das Sie ersetzen möchten.

HINWEIS: Die Option **Generate Replacement License for RMA Device** dient nur für den Austausch von RMA-Hardware. Sie kann nicht verwendet werden, um einen versehentlich erstellten Lizenzschlüssel zu ersetzen (wenn z. B. mit einem Autorisierungscode ein Lizenzschlüssel für ein IVE erstellt wurde, für das die Lizenz ursprünglich nicht erworben wurde).

---

4. Führen Sie auf der Seite **Generate Licenses** folgende Schritte aus:

   - Wenn Sie einen Lizenzschlüssel für nur ein IVE erstellen, geben Sie die Lizenzierungshardware-ID und mindestens einen Autorisierungscode in die entsprechenden Felder ein.

   - Wenn Sie Lizenzschlüssel für mehrere IVEs gleichzeitig erstellen möchten, klicken Sie auf **Generate License Keys for Multiple SSL VPN Devices**, und folgen Sie den Anweisungen auf dem Bildschirm, um die Excel-Datei zum Generieren der Lizenzschlüssel zu erstellen.

5. Klicken Sie auf **Generate**.

   Die Seite **Confirm License Information** wird mit einer Zusammenfassung der an das Lizenzverwaltungssystem gesendeten Informationen angezeigt.

6. Überprüfen Sie, ob die Informationen korrekt sind, und klicken Sie dann auf **Generate License**.

   Die Seite **Generate License SSL VPN** wird geöffnet. Sie enthält eine Zusammenfassung Ihrer Lizenzschlüssel und einen Link, über den Sie die Details der neuen Lizenzschlüssel anzeigen können.

7. Klicken Sie auf **Download/Email**, und geben Sie das gewünschte Dateiformat und die Übertragungsmethode an, mittels der Sie Ihre neuen Lizenzschlüssel erhalten möchten.

Gehen Sie folgendermaßen vor, nachdem Sie die Lizenzschlüssel heruntergeladen oder per E-Mail erhalten haben:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Licensing** aus.

2. Klicken Sie auf die Verknüpfung **license agreement**. Lesen Sie die Lizenzvereinbarung. Wenn Sie mit den Bestimmungen einverstanden sind, fahren Sie mit dem nächsten Schritt fort.

3. Geben Sie Ihre Lizenzschlüssel ein, und klicken Sie auf **Save Changes**.

Aktualisieren von IVE-Lizenzschlüsseln

Wenn Sie eine Remote Access 500-, Secure Access 1000-, Secure Access 3000-, Secure Access 5000- oder Secure Access FIPS-Appliance verwenden und Ihre Lizenzschlüssel nach dem Aktualisieren des Abbilds auf Ihrem auf Version 5.1 oder höher aktualisieren möchten, müssen Sie das folgende Verfahren ausführen, um die neuen Lizenzschlüssel zu erstellen und einzugeben. Da das IVE vorhandene Lizenzinformationen bei der Aktualisierung beibehält, müssen nur für alle erworbenen Lizenzaktualisierungen neue Lizenzschlüssel überprüft und erstellt werden. Abbildung 29 auf Seite 159 zeigt eine Übersicht der wichtigsten Schritte des Lizenzgenerierungsprozesses.

HINWEIS: Wenn Sie Ihre Lizenzschlüssel auf einem älteren aktualisieren, speichert das Juniper Networks-Lizenzverwaltungssystem sowohl Informationen über die neuen erstellten Lizenzschlüssel als auch über alle zukünftigen Lizenzschlüssel, die Sie erwerben und im eingeben. Sie können nicht auf Details zu älteren Lizenzschlüsseln zugreifen. Juniper Networks kann keine Lizenzschlüsselinformationen für Softwareversionen vor Version 5.1 überprüfen. Wenden Sie sich über den „Case Manager“ im Customer Support Center an den Kundendienst von Juniper, wenn Sie Ihre Lizenzinformationen versehentlich gelöscht haben:

- 1-800-638-8296 (USA und Kanada)
- 1-408-745-9500 (International)

Der Kundendienst von Juniper öffnet in Ihrem Namen einen Support-Fall und erstellt einen Datensatz der verlorenen Lizenzschlüssel.

So aktualisieren Sie Ihre IVE-Lizenzschlüssel:

1. Vergewissern Sie sich, dass Sie Ihre Lizenzierungshardware-ID und Autorisierungscodes zur Hand haben.

   Die *Lizenzierungshardware*-ID des IVE wird über den Menüoptionen in der seriellen Konsole und unten in der Administrator-Webkonsole angezeigt.

   Wenn Sie die Software und die Lizenzschlüssel Ihres IVE aktualisieren, erhalten Sie *Autorisierungscodes* für die zusätzlichen Funktionslizenzen von dem Händler, bei dem Sie das IVE ursprünglich erworben haben.

2. Navigieren Sie zum Juniper Networks-Lizenzverwaltungssystem unter https://www.juniper.net/generate_license.

HINWEIS: Das Juniper Networks-Lizenzverwaltungssystem enthält einen Zugriffspunkt, über den Sie detaillierte Informationen zu Juniper Networks-Lizenzen abrufen können. Dies beinhaltet auch alle für Sie und Ihre Firma registrierten Lizenzen und alle Lizenzen, die derzeit spezifischen Lizenzierungshardware-IDs zugeordnet sind.

Sie benötigen eine gültige Benutzer-ID und ein gültiges Kennwort für das Juniper Networks Customer Support Center, um an dieser Stelle auf die Informationen zuzugreifen. Anmeldeinformationen für das Juniper Networks Customer Support Center erhalten Sie über die Customer Support Center-Website unter https://www.juniper.net/customers/support/.

---

3. Klicken Sie auf den Link **Secure Access SSL VPN**, um neue IVE-Lizenzschlüssel zu generieren, oder klicken Sie auf **Generate Replacement License for RMA Device**, um basierend auf einer vorhandenen Lizenz eine Lizenz für ein IVE zu erstellen, das Sie ersetzen möchten.

HINWEIS: Die Option **Generate Replacement License for RMA Device** dient nur für den Austausch von RMA-Hardware. Sie kann nicht verwendet werden, um einen versehentlich erstellten Lizenzschlüssel zu ersetzen (wenn z. B. mit einem Autorisierungscode ein Lizenzschlüssel für ein IVE erstellt wurde, für das die Lizenz ursprünglich nicht erworben wurde).

---

4. Führen Sie auf der Seite **Generate Licenses** folgende Schritte aus:

   - Wenn Sie einen Lizenzschlüssel für nur ein IVE erstellen, geben Sie die Lizenzierungshardware-ID und mindestens einen Autorisierungscode in die entsprechenden Felder ein.

   - Wenn Sie Lizenzschlüssel für mehrere IVEs gleichzeitig erstellen möchten, klicken Sie auf **Generate License Keys for Multiple SSL VPN Devices**, und folgen Sie den Anweisungen auf dem Bildschirm, um die Excel-Datei zum Generieren der Lizenzschlüssel zu erstellen.

5. Klicken Sie auf **Generate**.

6. Geben Sie die Seriennummer des IVE in das Feld **Serial Number** ein. Wenn Sie die Seriennummer des IVE an der entsprechenden Eingabeaufforderung nicht eingeben, verwendet das Lizenzgenerierungsportal automatisch die in Schritt 4 eingegebene Lizenzierungshardware-ID.

7. Klicken Sie erneut auf **Generate**.

   Die Seite **Confirm License Information** wird mit einer Zusammenfassung der an das Lizenzverwaltungssystem gesendeten Informationen angezeigt.

8. Überprüfen Sie, ob die Informationen korrekt sind, und klicken Sie dann auf **Generate License**.

Die Seite **Generate License SSL VPN** wird geöffnet. Sie enthält eine Zusammenfassung Ihrer Lizenzschlüssel und einen Link, über den Sie die Details der neuen Lizenzschlüssel anzeigen können.

9. Klicken Sie auf **Download/Email**, und geben Sie das gewünschte Dateiformat und die Übertragungsmethode an, mittels der Sie Ihre neuen Lizenzschlüssel erhalten möchten.

Gehen Sie folgendermaßen vor, nachdem Sie die Lizenzschlüsselaktualisierungen heruntergeladen oder per E-Mail erhalten haben:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Licensing** aus.

2. Klicken Sie auf die Verknüpfung **license agreement**. Lesen Sie die Lizenzvereinbarung. Wenn Sie mit den Bestimmungen einverstanden sind, fahren Sie mit dem nächsten Schritt fort.

3. Geben Sie die Lizenzschlüssel ein, und klicken Sie auf **Save Changes**.

Seite „Security“

Über die Seite **System > Configuration > Security** können Sie die Standardsicherheitseinstellungen für das IVE festlegen. Wir empfehlen, die Standardsicherheitseinstellungen zu verwenden, die höchste Sicherheit bereitstellen. Falls die Benutzer bestimmte Browser nicht verwenden oder auf bestimmte Webseiten nicht zugreifen können, müssen Sie diese Einstellungen jedoch möglicherweise ändern. Zudem können Sie Sperroptionen konfigurieren, um das IVE und Back-End-Systeme vor DOS-/DDOS-/Kennwortermittlungsangriffen über dieselbe IP-Adresse zu schützen.

Festlegen von systemweiten Sicherheitsoptionen

Wenn bei Benutzern beim Zugriff auf bestimmte Webseiten Browserprobleme auftreten, müssen Sie ggf. Folgendes anpassen:

- **Zulässige SSL- und TLS-Version** – Legen Sie Verschlüsselungsanforderungen für IVE-Benutzer fest. (Das IVE erfordert standardmäßig SSL-Version 3 und TLS.) Sie können Benutzer von älteren Browsern mit SSL Version 2 dazu auffordern, ihre Browser zu aktualisieren oder die IVE-Einstellung ändern, damit SSL Version 2 und Version 3 sowie TLS zulässig sind.

- **Zulässige Verschlüsselungsstärke** – Das IVE erfordert standardmäßig 128-Bit-Verschlüsselung. Bei Bedarf können Sie für das IVE die 168-Bit-Verschlüsselung einstellen. In älteren Browsern, die vor der Änderung des US-Exportgesetzes im Jahr 2000 entwickelt wurden, das bis dahin für den internationalen Export eine Verschlüsselungsstärke von 40 Bit vorschrieb, wird u. U. noch die 40-Bit-Verschlüsselung verwendet. Sie können entweder den Benutzern mitteilen, dass diese eine Aktualisierung auf einen Browser mit 128-Bit-Verschlüsselung vornehmen sollen, oder die erforderliche Verschlüsselungsstärke ändern, so dass auch die 40-Bit-Verschlüsselung zulässig ist.

HINWEIS: Bei Verwendung von 168-Bit-Verschlüsselung für das IVE zeigen manche Webbrowser möglicherweise immer noch 128-Bit-Verschlüsselung an (das goldene Schloss auf der Statusleiste des Browsers), auch wenn es sich um 168-Bit-Verbindung handelt. Dabei kann es sich um eine Funktionsbeschränkung des Browsers handeln.

- **Delete all cookies at session termination** – Das IVE legt aus praktischen Gründen auf dem Computer des Benutzers permanente Cookies fest, z. B. das Cookie für den letzten Bereich und das Cookie für den letzten Anmelde-URL. Wenn Sie mehr Sicherheit oder Datenschutz wünschen, können Sie das Festlegen dieser Cookies verhindern.

Konfigurieren von Sperroptionen

Die folgenden **Sperroptionen** können konfiguriert werden, um das IVE und andere Systeme vor DoS- (Denial of Service), DDoS- (Distributed Denial of Service) und Kennwortermittlungsangriffen über dieselbe IP-Adresse zu schützen:

- **Rate** – Geben Sie die zulässige Anzahl von fehlgeschlagenen Anmeldeversuchen pro Minute an.

- **Attempts** – Geben Sie die maximal zulässige Anzahl von fehlgeschlagenen Anmeldeversuchen an, bevor die erste Sperre ausgelöst wird. Das IVE bestimmt den maximalen anfänglichen Zeitraum (in Minuten) für fehlgeschlagene Anmeldeversuche, indem es die angegebene Anzahl von Versuchen durch die Rate dividiert. 180 Versuche dividiert durch eine Rate von 3 ergibt z. B. einen Anfangszeitraum von 60 Minuten. Schlagen innerhalb von 60 Minuten (oder weniger) mehr als 180 Anmeldeversuche fehl, sperrt das IVE die für den fehlgeschlagenen Anmeldeversuch verwendete IP-Adresse.

- **Lockout period** – Legen Sie die Anzahl von Minuten fest, während der das IVE die IP-Adresse sperren soll.

Das IVE reagiert schnell auf einen fortbestehenden Angriff und lockert die Beschränkungen dann nach und nach, wenn der Angriff nachlässt. Nachdem eine IP-Adresse gesperrt wurde, stellt das IVE den vorherigen Zustand schrittweise wieder her, indem es die **Rate** beibehält. Wenn die aktuelle Fehlerrate seit der letzten Sperre den angegebenen Wert für **Rate** überschreitet, sperrt das IVE die IP-Adresse erneut. Ist die Fehlerrate während des mit **Attempts/Rate** ermittelten Zeitraums geringer als der angegebene Wert für **Rate**, stellt das IVE den ursprünglichen Überwachungsstatus wieder her.

Wenn Sie z. B. die folgenden Einstellungen für die **Sperroptionen** verwenden, sperrt das IVE die IP-Adresse für die unten gezeigten Zeiträume.

- **Rate** = 3 fehlgeschlagene Anmeldeversuche/Minute
- **Attempts** = maximal 180 im Anfangszeitraum von 60 Minuten (180/3)
- **Lockout period** = 2 Minuten

1. Während eines Zeitraums von drei Minuten erfolgen 180 fehlgeschlagene Anmeldeversuche von derselben IP-Adresse. Da der angegebene Wert für **Attempts** schneller erreicht wird als der zulässige Anfangszeitraum von 60 Minuten (180/3) erlaubt, sperrt das IVE die IP-Adresse für zwei Minuten (4. und 5. Minute).
2. In der 6. Minute hebt das IVE die Sperre der IP-Adresse auf, und es verwendet wieder die Rate von 3 fehlgeschlagenen Anmeldeversuchen/Minute. In der 6. und 7. Minute beträgt die Anzahl von fehlgeschlagenen Versuchen 2 pro Minute, so dass das IVE die IP-Adresse nicht sperrt. Wenn die Anzahl von fehlgeschlagenen Anmeldeversuchen jedoch in der 8. Minute auf 5 steigt und somit eine Gesamtanzahl von 9 fehlgeschlagenen Versuchen in 3 Minuten entsteht, sperrt das IVE die IP-Adresse erneut für 2 Minuten (9. und 10. Minute).
3. In der 11. Minute hebt das IVE die Sperre der IP-Adresse auf, und es verwendet wieder die Rate von 3 fehlgeschlagenen Anmeldeversuchen/Minute. Bleibt die Rate während eines Zeitraums von 60 Minuten unter einem Durchschnitt von 3/Minute stellt das IVE den ursprünglichen Überwachungsstatus wieder her.

HINWEIS: Für neue Systeme sind alle Optionen standardmäßig *deaktiviert*.

Registerkarten „Certificates“

Verwenden Sie die folgenden **Certificates**-Unterregisterkarten zum Hochladen von Server-, Client- und Codesignaturzertifikaten in das IVE, Herunterladen von Zertifikaten vom IVE, Erneuern von Zertifikaten, Löschen von Zertifikaten, Erstellen von Zertifikatssignaturanforderungen (CSR) für neue Zertifikate, Importieren von signierten Zertifikaten aus einer CSR, Aktivieren der CRL-Prüfung und Anzeigen von Zertifikatdetails.

- „Registerkarte „IVE Certificates““ auf Seite 166
- „Registerkarte „Trusted Client CAs““ auf Seite 170
- „Registerkarte „Trusted Server CAs““ auf Seite 179
- „Registerkarte „Code-Signing Certificates““ auf Seite 181

Registerkarte „IVE Certificates“

Das IVE unterstützt X.509-Serverzertifikate in DER- und PEM-Verschlüsselungsformaten (Dateierweiterungen .cer, .crt, .der und .pem) sowie im PKCS #12-Format (Dateierweiterungen.pfx und .p12).

Die Registerkarte **System > Configuration > Certificates > IVE Certificates** kann für folgende Aufgaben verwendet werden: Importieren eines Stammzertifikats und eines privaten Schlüssels, Importieren eines Zwischenzertifikats, Erstellen einer Zertifikatssignaturanforderung (CSR) und Importieren eines aus einer CSR erstellten Zertifikats.

Importieren eines vorhandenen Stammzertifikats und eines privaten Schlüssels

Sie können Webserverzertifikate von Servern wie Apache, IIS, Sun ONE (früher iPlanet) oder Netscape erstellen und das Zertifikat dann in das IVE importieren. Zum Exportieren eines digitalen Serverzertifikats und eines Schlüssels befolgen Sie die zu dem Webserver vorhandenen Anweisungen zum Exportieren von Zertifikaten. Importieren Sie anschließend diese Dateien über die Registerkarte **Server Certificates**.

So importieren Sie ein vorhandenes Server-Stammzertifikat und einen privaten Schlüssel:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > IVE Certificates**.
2. Klicken Sie auf **Import Certificate & Key**.
3. Wählen Sie das entsprechende Formular für den Import des Zertifikats aus:
   - Falls das Zertifikat und der Schlüssel in einer Datei enthalten sind, verwenden Sie das Formular **If certificate file includes private key**.
   - Handelt es sich bei dem Zertifikat und dem Schlüssel um separate Dateien, verwenden Sie das Formular **If certificate and private key are separate files**.
   - Wenn das Zertifikat und der Schlüssel in einer IVE-Konfigurationsdatei enthalten sind, verwenden Sie das Formular **Import via IVE configuration file**. Bei Auswahl dieser Option importiert das IVE alle in der Konfigurationsdatei angegebenen Zertifikate in die Seite **IVE Certificates** (einschließlich privater Schlüssel und ausstehender CSRs, nicht jedoch der zugehörigen Portzuordnungen).
4. Wechseln Sie im entsprechenden Formular zu der Datei mit dem Zertifikat und dem Schlüssel. Wenn die Datei verschlüsselt ist, geben Sie den Kennwortschlüssel ein.
5. Klicken Sie auf **Import**.

Importieren eines vorhandenen Zwischenzertifikats

Sie können den Datenverkehr sichern, indem Sie eine von einer vertrauten Zertifizierungsstelle ausgegebene Zertifikatkette verwenden. In diesem Fall müssen Sie sicherstellen, dass die gesamte Zertifikatkette im IVE und im Webbrowser enthalten ist, wie unter „Serverzwischenzertifikate“ auf Seite 66 beschrieben.

Wenn Sie Zertifikate durch das IVE installieren, können Sie dazu eine beliebige Reihenfolge verwenden. Das IVE unterstützt das Hochladen von Zwischen-CAs in eine PEM-Datei.

So importieren Sie ein Server-Zwischenzertifikat und einen privaten Schlüssel:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > IVE Certificates**.
2. Klicken Sie oben auf der Seite auf den Link **Intermediate IVE CAs**.
3. Klicken Sie auf **Import CA certificate**.
4. Navigieren Sie zum Zertifizierungsstellenzertifikat, das Sie auf das IVE hochladen möchten, und klicken Sie auf **Import Certificate**.

Importieren eines erneuerten Zertifikats, das den vorhandenen privaten Schlüssel verwendet

Sie können ein Serverzertifikat auf zwei Arten erneuern:

- **Neue Zertifikatssignaturanforderung an eine Zertifizierungsstelle senden** – Dieses Verfahren zur Erneuerung eines Zertifikats ist sicherer, da die Zertifizierungsstelle ein neues Zertifikat und einen neuen privaten Schlüssel generiert und dabei die Gültigkeit des älteren privaten Schlüssels aufhebt. Zur Verwendung dieser Erneuerungsmethode müssen Sie zuerst über die Webkonsole eine Zertifikatsignaturanforderung erstellen. Weitere Informationen finden Sie unter „Erstellen einer Zertifikatssignaturanforderung für ein neues Zertifikat“ auf Seite 169.
- **Erneuerung basierend auf der zuvor an die Zertifizierungsstelle gesendeten Zertifikatssignaturanforderung anfordern** – Dieses Verfahren zur Erneuerung eines Zertifikats ist weniger sicher, da die Zertifizierungsstelle ein Zertifikat generiert, das den vorhandenen privaten Schlüssel verwendet.

HINWEIS: Wenn Sie ein erneuertes Zertifikat anfordern, müssen Sie Ihre ursprüngliche Zertifikatssignaturanforderung erneut senden, um sicherzustellen, dass die Zertifizierungsstelle über einen Datensatz für die Zertifikatssignaturanforderung verfügt, die Sie für Ihr aktuelles Zertifikat gesendet haben.

So importieren Sie ein erneuertes Serverzertifikat, das den vorhandenen privaten Schlüssel verwendet

1. Befolgen Sie die Anweisungen der Zertifizierungsstelle zur Erneuerung eines Zertifikats, das Sie zuvor dort erworben haben.

HINWEIS: Achten Sie darauf, dass Sie dieselben Informationen wie in der ursprünglichen Zertifikatsignaturanforderung eingeben. Anhand dieser Informationen erstellt die Zertifizierungsstelle ein neues Zertifikat, das dem vorhandenen Schlüssel entspricht.

2. Wählen Sie in der Webkonsole **System > Configuration > Certificates > IVE Certificates**.
3. Wenn Sie ein Zwischenzertifikat erneuern möchten, klicken Sie oben auf der Seite auf den Link **Intermediate IVE CAs**.

4. Klicken Sie auf den Link für das zu erneuernde Zertifikat.

5. Klicken Sie auf **Renew Certificate**.

6. Navigieren Sie im Formular **Renew the Certificate** zu der erneuerten Zertifikatsdatei, geben Sie das Kennwort für den Zertifizierungsschlüssel ein, und klicken Sie auf **Import**.

Herunterladen eines Serverzertifikats vom IVE

Auf der Seite **Server Certificates** können Sie auf einfache Weise das Zertifikat der IVE-Appliance herunterladen.

So laden Sie ein Serverzertifikat vom IVE herunter:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > IVE Certificates**.

2. Klicken Sie auf den Link für das zu speichernde Zertifikat.

3. Klicken Sie auf **Download**.

4. Navigieren Sie zu dem Speicherort, an dem Sie das Zertifikat speichern möchten, und klicken Sie auf **Save**.

Erstellen einer Zertifikatssignaturanforderung für ein neues Zertifikat

Falls Ihr Unternehmen über kein digitales Zertifikat für die Webserver verfügt, können Sie über die Webkonsole eine Zertifikatssignaturanforderung erstellen und diese dann zur Verarbeitung an eine Zertifizierungsstelle senden. Wenn Sie über die Webkonsole eine Zertifikatssignaturanforderung erstellen, wird lokal ein privater Schlüssel erstellt, der der Zertifikatssignaturanforderung entspricht. Falls Sie die Zertifikatssignaturanforderung löschen, wird diese Datei ebenfalls gelöscht. Es ist dann nicht mehr möglich, ein über die Zertifikatssignaturanforderung erstelltes signiertes Zertifikat zu installieren.

HINWEIS: Senden Sie nur jeweils eine Zertifikatssignaturanforderung an eine Zertifizierungsstelle. Andernfalls fallen u. U. doppelte Gebühren an. Sie können Details zu zuvor gesendeten, ausstehenden Anforderungen anzeigen, indem Sie auf die Verknüpfung **Certificate Signing Request Details** auf der Registerkarte **Server Certificates** klicken.

So erstellen Sie eine Zertifikatssignaturanforderung

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > IVE Certificates**.

2. Klicken Sie auf **New CSR**.

3. Geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Create CSR**.

4. Folgen Sie den Anweisungen auf dem Bildschirm. Darin wird neben dem Sendeverfahren erläutert, welche Informationen an die Zertifizierungsstelle gesendet werden müssen.

5. Wenn Sie von der Zertifizierungsstelle ein signiertes Zertifikat erhalten, importieren Sie anhand der folgenden Anweisungen die Zertifikatdatei.

HINWEIS: Wenn Sie eine Zertifikatssignaturanforderung bei einer Zertifizierungsstelle einreichen, werden Sie u. U. dazu aufgefordert, entweder den Typ des Webservers anzugeben, auf dem das Zertifikat erstellt wurde, oder den Typ des Webservers, für den das Zertifikat bestimmt ist. Wählen Sie **apache** aus (falls mehrere Optionen mit „apache“ verfügbar sind, wählen Sie eine beliebige aus). Wählen Sie außerdem, falls Sie zur Auswahl des Formats des herunterzuladenden Zertifikats aufgefordert werden, das Standardformat aus.

Importieren eines signierten Zertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde

Wenn Sie über die Webkonsole eine Zertifikatssignaturanforderung erstellen, zeigt das IVE auf der Registerkarte **Server Certificates** einen Link **Pending CSR** für die Zertifikatssignaturanforderung an, bis Sie das von der Zertifizierungsstelle ausgestellte signierte Serverzertifikat importieren.

So importieren Sie ein signiertes Serverzertifikat, das anhand einer Zertifikatssignaturanforderung erstellt wurde

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > IVE Certificates**.

2. Klicken Sie unter **Certificate Signing Requests** auf den Link **Pending CSR** für das signierte Zertifikat.

3. Navigieren Sie unter **Import signed certificate** zu der Zertifikatdatei, die Sie von der Zertifizierungsstelle erhalten haben, und klicken Sie dann auf **Import**.

Registerkarte „Trusted Client CAs“

Die Registerkarte **System > Configuration > Certificates > Trusted Client CAs** dient zum Ausführen einer Reihe von Aufgaben für den Import, die Konfiguration und die Verwaltung von Client-Zertifizierungsstellenzertifikaten im IVE. Dieser Abschnitt ist in folgende Themen untergliedert:

- „Hochladen von Zertifikaten der vertrauten Clientzertifizierungsstelle in das IVE“ auf Seite 171
- „Festlegen von Attributen für das vertrauenswürdige Client-Zertifizierungsstellenzertifikat“ auf Seite 173
- „Festlegen von OCSP-Optionen“ auf Seite 175
- „Festlegen von OCSP-Responderoptionen“ auf Seite 176
- „Festlegen von CDP-Optionen“ auf Seite 177

- „Aktivieren eines Clientzertifikats für Benutzerbereiche“ auf Seite 179

HINWEIS: Das IVE unterstützt X.509-Zertifizierungsstellenzertifikate im DER- und PEM-Verschlüsselungsformat.

Hochladen von Zertifikaten der vertrauten Clientzertifizierungsstelle in das IVE

Wenn Sie bestimmen, dass Benutzer zum Anmelden am IVE ein clientseitiges Zertifikat bereitstellen müssen, müssen Sie das entsprechende Zertifikat der Zertifizierungsstelle auf das IVE hochladen. Sie können CA-Zertifikate manuell hochladen oder das IVE zum automatischen Hochladen von CA-Zertifikate konfigurieren. Das IVE verwendet das hochgeladene Zertifikat zum Überprüfen, ob das vom Browser bereitgestellte Zertifikat gültig ist. Zudem können Sie festlegen, ob CA-Zertifikate zur Überprüfung automatisch importiert werden sollen, und Sie können die CRL/OCSP-Abrufmethode angeben, die das IVE beim automatischen Importieren der CA-Zertifikate verwendet. Weitere Informationen zu CRL und OCSP finden Sie unter „CAs vertrauter Clients“ auf Seite 67.

HINWEIS:

- Bei Verwendung clientseitiger Zertifikate ist dringend zu empfehlen, die Benutzer anzuweisen, ihre Webbrowser nach dem Abmelden vom IVE zu schließen. Andernfalls können andere Benutzer über deren geöffnete Browsersitzungen auf durch Zertifikate geschützte Ressourcen auf dem IVE ohne erneute Authentifizierung zugreifen. (Nach dem Laden eines clientseitigen Zertifikats werden die Anmeldedaten und der private Schlüssel des Zertifikats von Internet Explorer zwischengespeichert. Diese Informationen bleiben in den Browsern zwischengespeichert, bis der Browser vom Benutzer geschlossen wird (in manchen Fällen, bis die Arbeitsstation neu gestartet wird). Ausführliche Informationen finden Sie unter: http://support.microsoft.com/?kbid=290345.) Sie können die Benutzer daran erinnern, ihren Browser zu schließen, indem Sie die Meldung für die Abmeldung auf der Registerkarte **System > Signing In > Sign-in Pages** ändern.

- Durch das Hochladen eines Zertifizierungsstellenzertifikats in das IVE wird die clientseitige SSL-Authentifizerung nicht aktiviert. Sie müssen entweder einen Zertifikatserver verwenden oder auf der Seite **Administrators/Users > Authentication > [Bereich] > Authentication Policy > Certificate** der Webkonsole Zertifikateinschränkungen aktivieren, um die clientseitige SSL-Authentifizierung zu aktivieren.

- In einer Secure Access 700-Appliance kann nur ein Zertifizierungsstellenzertifikat in das IVE importiert werden.

- Beim Hochladen einer Zertifikatkette auf das IVE müssen Sie entweder beginnend mit dem Stammzertifikat die Zertifikate einzeln in absteigender Reihenfolge installieren (DER- oder PEM-Dateien) oder eine einzelne Datei auf das IVE hochladen, die die gesamte Zertifikatkette enthält (nur PEM-Dateien). Durch Verwenden einer dieser Methoden stellen Sie sicher, dass das IVE die Zertifikate in der richtigen Reihenfolge miteinander verknüpft.

So führen Sie den Import automatisch durch und legen Sie Optionen für ein vertrauenswürdiges Client-Zertifizierungsstellenzertifikat im IVE fest:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > Trusted Client CAs**.

2. Klicken Sie auf **Auto-import options**. Die Seite **Auto-import options** wird angezeigt.

3. Klicken Sie auf **Auto-import Trusted CAs**.

4. Geben Sie unter **Client certificate status checking** die Methode an, die das IVE zum Überprüfen des Clientzertifikatstatus verwendet:

   - **None** – Gibt an, dass das IVE dieses vertrauenswürdige Clientzertifikat nicht überprüfen soll.

   - **Use OCSP** – Gibt an, dass das IVE bei Bedarf die OCSP-Methode verwenden und das Clientzertifikat in Echtzeit überprüfen soll. Nachdem Sie diese Option ausgewählt haben, können Sie wie unter „Festlegen von OCSP-Optionen“ auf Seite 175 beschrieben Optionen für OCSP festlegen.

   - **Use CRLs** – Gibt an, dass das IVE CRLs zum Überprüfen des Clientzertifikats verwenden soll. Nachdem Sie diese Option ausgewählt haben, können Sie wie unter „Festlegen von CDP-Optionen“ auf Seite 177 beschrieben Optionen für OCSP festlegen.

   - **Use OCSP with CRL fallback** – Gibt an, dass das IVE sofern möglich die OCSP-Überprüfungsmethode verwenden soll, bei einem Fehlschlag der OCSP-Methode (z. B. wenn der Link zum OCSP-Responder nicht funktioniert) Clientzertifikate aber anhand von CRLs validieren soll. Nachdem Sie diese Option ausgewählt haben, können Sie wie unter „Festlegen von OCSP-Optionen“ auf Seite 175 beschrieben Optionen für OCSP und wie unter „Festlegen von CDP-Optionen“ auf Seite 177 beschrieben Optionen für CDP festlegen.

5. Wählen Sie unter **CDP(s)/OCSP responder** in der entsprechenden Dropdownliste die CRL/OCSP-Abrufmethode aus:

   - **None** – Das IVE verwendet keine CRL/OCSP-Abrufmethode.

   - **From client certificate** – Das IVE verwendet eine im Clientzertifikat enthaltene CRL/OCSP-Abrufmethode.

   - **From trusted CA certificates** – Das IVE verwendet eine im vertrauenswürdigen Client-Zertifizierungsstellenzertifikat enthaltene CRL/OCSP-Abrufmethode.

6. Aktivieren Sie die Option **Verify imported CA certificates**, wenn das IVE die CRL überprüfen soll, von der das Zertifikat ausgestellt wird.

7. Klicken Sie auf **Save**.

So laden Sie Zertifizierungsstellenzertifikate manuell auf das IVE hoch:

1. Installieren Sie ein clientseitiges Zertifikat über den Browser des Benutzers. Hilfe dazu können Sie den Anweisungen zu dem Browser entnehmen.

2. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Trusted Client CAs** aus.

3. Klicken Sie auf **Import CA Certificate**. Die Seite **Import Trusted Client CA** wird angezeigt.

4. Navigieren Sie zum Zertifizierungsstellenzertifikat, das Sie auf das IVE hochladen möchten, und klicken Sie auf **Import Certificate**. Die Seite **Trusted Client CA** wird mit den Zertifikatattributen angezeigt. Zu diesen Attributen zählen die für das Zertifikat aktivierte Zertifikatstatusprüfung und eine Angabe dazu, ob das IVE zur Überprüfung von vertrauenswürdigen Client-CAs konfiguriert ist.

5. Klicken Sie auf **Save**.

   Nachdem Sie das CA-Zertifikat manuell importiert haben, können Sie wie unter „Festlegen von Attributen für das vertrauenswürdige Client-Zertifizierungsstellenzertifikat“ auf Seite 173 beschrieben CA-Zertifikatattribute angeben.

Festlegen von Attributen für das vertrauenswürdige Client-Zertifizierungsstellenzertifikat

So legen Sie Attribute für das vertrauenswürdige Client-Zertifizierungsstellenzertifikat fest

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Trusted Client CAs** aus.

2. Klicken Sie auf das Zertifikat, das Sie anzeigen möchten. Die Seite **Trusted Client CA** wird mit allen Informationen über das von Ihnen ausgewählte Zertifikat angezeigt.

3. Verwenden Sie unter **Certificate** den Pfeil neben den folgenden Feldnamen, um Zertifikatdetails anzuzeigen:

   - **Issued To** – Name und Attribute der Einheit, für die das Zertifikat ausgestellt ist.

   - **Issued By** – Name und Attribute der Einheit, die das Zertifikat ausgestellt hat. Beachten Sie, dass der Wert dieses Feldes entweder dem Inhalt des Feldes **Issued To** (für Stammzertifikate) oder dem des Feldes **Issued To** des nächsten Zertifikats weiter oben in der Kette (für Zwischenzertifikate) entsprechen sollte.

   - **Valid Dates** – Gültigkeitszeitraum des Zertifikats. Wenn Ihr Zertifikat abgelaufen ist, finden Sie diesbezügliche Anweisungen unter „Importieren eines erneuerten Zertifikats, das den vorhandenen privaten Schlüssel verwendet“ auf Seite 168.

- **Details** – Beinhaltet verschiedene Zertifikatdetails, darunter Version, Seriennummer, Signaturalgorithmus, CRL-Verteilungspunkte, den öffentlichen Schlüssel und dessen Algorithmustyp. Auch wenn das IVE im Feld **Details** einen CRL-Verteilungspunkt anzeigt, überprüft es den Sperrlisten-Verteilungspunkt nur dann, wenn Sie ihn aktivieren. Weitere Informationen finden Sie unter „Zertifikatsperrlisten“ auf Seite 69.

4. Wenn Sie das Zertifikat erneuern möchten:

   a. Klicken Sie auf **Renew Certificate**.

   b. Navigieren Sie zum Zertifizierungsstellenzertifikat, das Sie auf das IVE hochladen möchten, und klicken Sie auf **Import Certificate**.

5. Unter **CRL checking for client certificates** können Sie Details der CRL(s) anzeigen, die für dieses Zertifikat aktiviert ist bzw. sind:

   - **Enable** – Hier wird ein Häkchen angezeigt, wenn das IVE zur Verwendung der CRL von diesem Sperrlisten-Verteilungspunkt konfiguriert ist.

   - **CRL Distribution Points** – Position des CRL-Verteilungspunktes, anhand dessen die Clientzertifikate überprüft werden. In diesem Feld wird außerdem angezeigt, ob der letzte Versuch zum Herunterladen der CRL vom Sperrlisten-Verteilungspunkt erfolgreich war.

   - **Status** – Zeigt den Status der CRL („OK“, „No CRL“, „Expired“, „Download in progress“), die Größe der CRL und die Anzahl der in der CRL enthaltenen Sperrungen an.

   - **Last Updated** – Zeigt die Zeit an, zu der das IVE zuletzt eine CRL von dem angegebenen CRL-Verteilungspunkt heruntergeladen hat. Enthält außerdem eine Verknüpfung, mit der Sie die aktuelle Version der CRL des IVE speichern können.

   - **Next Update** – Zeigt die geplante Zeit an, zu der das IVE das nächste Mal eine CRL von dem angegebenen CRL-Verteilungspunkt herunterladen soll. Beachten Sie, dass sowohl in der CRL als auch auf der CRL-Konfigurationsseite des IVEs ein Intervall zum Herunterladen angegeben ist. Der hier angezeigte Wert ist der kleinere von beiden.

6. Geben Sie im Abschnitt **Client Certificate Status Checking** die Methode an, die das IVE zum Überprüfen des Clientzertifikats verwendet:

   - **None** – Gibt an, dass das IVE dieses vertrauenswürdige Clientzertifikat nicht überprüfen soll.

   - **Use OCSP** – Gibt an, dass das IVE bei Bedarf die OCSP-Methode verwenden und das Clientzertifikat in Echtzeit überprüfen soll. Nachdem Sie diese Option ausgewählt haben, können Sie wie unter „Festlegen von OCSP-Optionen“ auf Seite 175 beschrieben Optionen für OCSP festlegen.

   - **Use CRLs** – Gibt an, dass das IVE CRLs zum Überprüfen des Clientzertifikats verwenden soll. Nachdem Sie diese Option ausgewählt haben, können Sie wie unter „Festlegen von CDP-Optionen“ auf Seite 177 beschrieben Optionen für OCSP festlegen.

- **Use OCSP with CRL fallback** – Gibt an, dass das IVE sofern möglich die OCSP-Überprüfungsmethode verwenden soll, bei einem Fehlschlag der OCSP-Methode (z. B. wenn der Link zum OCSP-Responder nicht funktioniert) Clientzertifikate aber anhand von CRLs validieren soll. Nachdem Sie diese Option ausgewählt haben, können Sie wie unter „Festlegen von OCSP-Optionen“ auf Seite 175 beschrieben Optionen für OCSP und wie unter „Festlegen von CDP-Optionen“ auf Seite 177 beschrieben Optionen für CDP festlegen.

7. Aktivieren Sie die Option **Verify Trusted Client CA**, damit das IVE die vertrauenswürdige Client-CA überprüft.

8. Klicken Sie auf **Save Changes**.

Festlegen von OCSP-Optionen

Wenn Sie in Schritt 6 unter „Festlegen von Attributen für das vertrauenswürdige Client-Zertifizierungsstellenzertifikat“ auf Seite 173 die Option **Use OCSP** oder **Use OCSP with CRL fallback** ausgewählt haben, zeigt das IVE eine Liste bekannter OCSP-Responder an, und Sie können Optionen für den OCSP-Responder konfigurieren:

1. Löschen, aktivieren oder deaktivieren Sie die OCSP-Responderkonfiguration mit den Schaltflächen **Delete**, **Enable** bzw. **Disable**.

2. Klicken Sie auf **OCSP Options**, wenn Sie OCSP-Optionen konfigurieren möchten. Die Seite **OCSP Options** wird angezeigt.

3. Wählen Sie in der Dropdownliste **Use** den OCSP-Respondertyp aus, den das IVE zum Überprüfen vertrauenswürdiger Client-CAs verwendet:

   - **None** – Das IVE verwendet OCSP nicht, um den Status der von dieser CA ausgestellten Zertifikate zu überprüfen.

   - **Responder(s) specified in the CA certificate** – Das IVE verwendet in der importierten Client-CA angegebene OCSP-Responder für die Überprüfung. Wenn Sie diese Option auswählen, zeigt das IVE eine Liste der in der importierten CA angegebenen OCSP-Responder (sofern vorhanden) sowie das Datum und die Uhrzeit ihrer letzten Verwendung an.

   - **Responder(s) specified in the client certificates** – Das IVE verwendet während der Clientauthentifizierung angegebene OCSP-Responder für die Überprüfung. Wenn Sie diese Option auswählen, zeigt das IVE eine Liste bekannter OCSP-Responder (sofern vorhanden) sowie das Datum und die Uhrzeit ihrer letzten Verwendung an.

   - **Manually configured responders** – Das IVE verwendet primäre und sekundäre OCSP-Responder an den von Ihnen angegebenen Adressen.

4. Geben Sie im Abschnitt **Options** an, ob das IVE die Zertifikatüberprüfungsanfrage mit einem Bezeichner signiert und ob das IVE während der Überprüfung eine Ad-Hoc-Zahl verwendet.

HINWEIS: *Ad-Hoc-Zahlen* sind zufällige Daten, die das IVE in eine OCSP-Anfrage anschließt und der OCSP-Responder in der OCSP-Antwort zurückgibt. Das IVE vergleicht die Ad-Hoc-Zahl in der Anfrage und der Antwort, um sicherzustellen, dass die Antwort vom OCSP-Responder generiert wurde. Wenn die Zahlen nicht übereinstimmen, ignoriert das IVE die Antwort, und es sendet eine neue Anfrage. Ad-Hoc-Zahlen sind eine gebräuchliche Methode zur Verhinderung von Wiedergabeangriffen.

5. Klicken Sie auf **Save Changes**.

Festlegen von OCSP-Responderoptionen

So legen Sie Optionen für OCSP-Respondersignaturzertifikate für OCSP-Responder fest:

1. Klicken Sie in der Liste **OCSP responders** auf den Namen des zu konfigurierenden OCSP-Responder. Die Optionsseite für den OCSP-Responder wird angezeigt.

2. Navigieren Sie zum Netzwerkpfad oder lokalen Verzeichnisspeicherort eines **Responder Signer Certificate**. Dies ist das Zertifikat, das der OCSP-Responder zum Signieren der Antwort verwendet. Sie müssen das Respondersignaturzertifikat angeben, wenn das Signaturzertifikat nicht in der Antwort enthalten ist.

3. Wenn Sie die Verwendung eines OCSP-Responderzertifikats zulassen möchten, das mit dem Respondersignaturzertifikat übereinstimmt, aktivieren Sie das Kontrollkästchen **Trust Responder Certificate**.

4. Aktivieren Sie die Option **Revocation Checking**, um sicherzustellen, dass das vom IVE und OCSP-Responder verwendete Zertifikat nicht kürzlich gesperrt wurde. Diese Option hat nur dann eine Wirkung, wenn Sie in Schritt 6 unter „Festlegen von Attributen für das vertrauenswürdige Client-Zertifizierungsstellenzertifikat“ auf Seite 173 die Option **Use OCSP with CRL fallback** ausgewählt haben.

5. Geben Sie im Feld **Allow clock discrepancy** einen Diskrepanzwert für die Uhrzeit an, um mögliche Abweichungen der Zeitstempel des IVE und des OCSP-Responder zu berücksichtigen. Wenn die Abweichung erheblich ist, wird die Antwort des OCSP-Responder vom IVE einfach als veraltet oder abgelaufen eingestuft und ignoriert.

6. Klicken Sie auf **Save Changes**.

Festlegen von CDP-Optionen

Wenn Sie in Schritt 6 unter „Festlegen von Attributen für das vertrauenswürdige Client-Zertifizierungsstellenzertifikat“ auf Seite 173 die Option **Use CRLs** oder **Use OCSP with CRL fallback** ausgewählt haben, können Sie Zertifikatsperrlisten (CRL) aktivieren und regelmäßig von Sperrlisten-Verteilungspunkten (CDPs) herunterladen, um die Gültigkeit von Clientzertifikaten fortlaufend zu überprüfen.

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Trusted Client CAs** aus.

2. Klicken Sie auf die Verknüpfung, die dem Zertifikat entspricht, für das Sie die CRL-Überprüfung aktivieren möchten.

HINWEIS: Da das IVE die Aufteilung von Zertifikatsperrlisten unterstützt, werden unter **CRL distribution points** möglicherweise mehrere CRLs angezeigt. Dies ist darauf zurückzuführen, dass die aufgeteilten Abschnitte einer Sperrliste nicht einzeln genannt, sondern anhand des Sperrlisten-Verteilungspunkts angegeben werden, von dem sie abgeleitet wurden.

---

3. Klicken Sie auf **CRL Checking Options**. Die Seite **CRL Checking Options** wird angezeigt.

4. Geben Sie unter **CRL Distribution Points** an, wo das IVE Zugriffsinformationen für den Sperrlisen-Verteilungspunkt finden kann. Folgende Optionen stehen zur Verfügung:

   - **No CDP (no CRL Checking)** – Wenn Sie diese Option auswählen, überprüft das IVE von der Zertifizierungsstelle ausgestellte CRLs nicht. Deshalb müssen Sie keine Parameter für den Zugriff auf den Sperrlisten-Verteilungspunkt eingeben, der die CRL ausgestellt hat.

   - **CDP(s) specified in the Trusted CA Client** – Wenn Sie diese Option auswählen, überprüft das IVE das CRL-Verteilungspunktattribut im Zertifikat und zeigt die URIs der Sperrlisten-Verteilungspunkte an, die es auf der Seite **CRL Checking Options** findet. Wenn das Zertifizierungsstellenzertifikat nicht alle für den Zugriff auf den Sperrlisten-Verteilungspunkt benötigten Informationen enthält, geben Sie die zusätzlich erforderlichen Informationen an:

     - **CDP Server:** (nur LDAP) – Geben Sie den Standort des CDP-Servers ein. Geben Sie bei Verwendung des LDAP-Protokolls die IP-Adresse oder den Hostnamen ein (z. B. ldap.domain.com).

     - **CRL Attribute:** (nur LDAP) – Geben Sie das LDAP-Attribut für das Objekt ein, das die CRL enthält (z. B. CertificateRevocationList).

     - **Admin DN**, **Password**: (nur LDAP) – Wenn der CDP-Server keine anonyme Suche für die CRL zulässt, geben Sie den zur Authentifizierung am CDP-Server erforderlichen Administrator-DN und das Kennwort ein.

- **CDP(s) specified in client certificates** – Wenn das Clientzertifikat nicht alle für den Zugriff auf den Sperrlisten-Verteilungspunkt benötigten Informationen enthält, geben Sie die zusätzlich erforderlichen Informationen an:
  - **CDP Server** (nur LDAP) – Geben Sie den Standort des CDP-Servers ein. Geben Sie bei Verwendung des LDAP-Protokolls die IP-Adresse oder den Hostnamen ein (z. B. ldap.domain.com).
  - **CRL Attribute** (nur LDAP) – Geben Sie das LDAP-Attribut für das Objekt ein, das die CRL enthält (z. B. CertificateRevocationList).
  - **Admin DN**, **Password** (nur LDAP) – Wenn der CDP-Server keine anonyme Suche für die CRL zulässt, geben Sie den zur Authentifizierung am CDP-Server erforderlichen Administrator-DN und das Kennwort ein.
- **Manually configured CDP** – Wenn Sie diese Option auswählen, greift das IVE auf den angegebenen Sperrlisten-Verteilungspunkt zu. Geben Sie den URL des primären Sperrlisten-Verteilungspunktes (CDP) und optional den eines Sicherungs-CDP ein. Verwenden Sie für einen LDAP-Server folgende Syntax: ldap://Server/BaseDN?attribute?Scope?Filter. Geben Sie für einen Webserver den vollständigen Pfad zum CRL-Objekt ein. Beispiel: http://domain.com/CertEnroll/CompanyName%20CA%20Server.crl

  Wenn der CDP-Server keine anonyme Suche für die CRL gestattet, geben Sie Administrator-DN und das Kennwort ein, die zur Authentifizierung am CDP-Server erforderlich sind. (nur LDAP)

HINWEIS: Wenn Sie zum Herunterladen von CDPs eine Methode verwenden und dann eine andere Methode auswählen, löscht das IVE alle Sperrlisten-Verteilungspunkte von der Festplatte, die mit der ersten Methode heruntergeladen wurden.

5. Geben Sie im Feld **CRL Download Frequency** an, wie oft das IVE die CRL vom Sperrlisten-Verteilungspunkt herunterladen soll. Der zulässige Bereich ist 1 bis 9999 Stunden.
6. Klicken Sie auf **Save Changes**.
7. Wenn Sie die Gültigkeit Ihres Zertifizierungsstellenzertifikats (zusätzlich zu clientseitigen Zertifikaten) anhand der in den vorherigen Schritten angegebenen CRL überprüfen möchten, wählen Sie auf der Seite **Trusted Client CA** die Option **Verify Trusted Client CA** aus.

HINWEIS:

- Wenn Sie ein Zwischenzertifikat überprüfen möchten, müssen Sie sicherstellen, dass für alle Zertifizierungsstellenzertifikate, die sich in der Kette über dem Zwischenzertifikat befinden, CRLs verfügbar sind. Beim Überprüfen eines Zertifizierungsstellenzertifikats überprüft das IVE auch alle ausstellenden Zertifizierungsstellen oberhalb des Zertifikats in der Kette.

- Wenn Sie diese Option auswählen, aber die CRL-Überprüfung nicht aktivieren, überprüft das IVE das Zertifizierungsstellenzertifikat anhand des Sperrlisten-Verteilungspunktes für den Aussteller der Zertifizierungsstelle. Wenn für den Aussteller keine CRL aktiviert ist, schlägt die Benutzerauthentifizierung fehl.

8. Klicken Sie auf **Save Changes**. Das IVE lädt die CRL mit der von Ihnen angegebenen Methode herunter (falls möglich) und zeigt CRL-Überprüfungsdetails an (wie im folgenden Abschnitt beschrieben).

9. Klicken Sie auf der Seite **Trusted Client CA** auf **Update Now**, um die CRL manuell vom Sperrlisten-Verteilungspunkt herunterzuladen (optional).

Aktivieren eines Clientzertifikats für Benutzerbereiche

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Trusted Client CAs** aus.

2. Legen Sie fest, welche Bereiche das Zertifikat zum Authentifizieren von Benutzern verwenden sollen, und aktivieren Sie dann mit den Einstellungen auf der Registerkarte **Users > Authentication > [Bereich] > Authentication Policy > Certificate** das Zertifikat für diese Bereiche.

3. Legen Sie X.509-DN-Attribute (Distinguished Name) fest, die Benutzer zur Authentifizierung, zum Rollen- bzw. Ressourcenrichtlinienzugriff oder zum Aktivieren der Zertifikatauthentifizierung für Administratorbereiche zusätzlich zu Benutzerbereichen angeben müssen (optional).

Registerkarte „Trusted Server CAs“

Die Registerkarte **Trusted Server CAs** dient zum Hochladen von Zertifikaten der vertrauten Serverzertifizierungsstelle in das IVE, Erneuern von Zertifikaten der vertrauten Serverzertifizierungsstelle und Anzeigen von Zertifikatdetails.

Hochladen von Zertifikaten der vertrauten Serverzertifizierungsstelle in das IVE

Verwenden Sie die Registerkarte **System > Configuration > Certificates > Trusted Server CAs** zum Importieren der Zertifizierungsstellenzertifikate vertrauter Websites in das IVE. Das IVE unterstützt X.509-Zertifizierungsstellenzertifikate im Verschlüsselungsformat PEM (Base 64) und DER (binär). Geben Sie außerdem an, wie das IVE verfährt, wenn ein Benutzer versucht, auf eine nicht vertraute Website zuzugreifen. Weitere Informationen finden Sie unter „Zertifikateinschränkungen“ auf Seite 421.

So laden Sie Zertifizierungsstellenzertifikate auf das IVE hoch:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Trusted Server CAs**.
2. Klicken Sie auf **Import Trusted Server CA**.
3. Navigieren Sie zum Zertifizierungsstellenzertifikat, das Sie auf das IVE hochladen möchten, und klicken Sie auf **Import Certificate**.

Erneuern eines Zertifikats der vertrauten Serverzertifizierungsstelle

Erneuert eine Ihrer vertrauten Websites ihr Zertifikat, müssen Sie das erneuerte Zertifikat auch ins IVE laden.

So importieren Sie ein erneuertes Zertifizierungsstellenzertifikat in das IVE:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Trusted Server CAs**.
2. Klicken Sie auf die Verknüpfung, die dem zu erneuernden Zertifikat entspricht.
3. Klicken Sie auf **Renew Certificate**.
4. Navigieren Sie zum Zertifizierungsstellenzertifikat, das Sie auf das IVE hochladen möchten, und klicken Sie auf **Import Certificate**.

Löschen eines Zertifikats der vertrauten Serverzertifizierungsstelle

Sie können jedes Zertifikat einer im IVE installierten vertrauten Serverzertifizierungsstelle löschen, einschließlich vorinstallierter Zertifikate für Internet Explorer 6 und Windows XP Service Pack 2.

So löschen Sie ein Zertifikat einer vertrauten Serverzertifizierungsstelle aus dem IVE:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Trusted Server CAs**.
2. Aktivieren Sie das Kontrollkästchen neben dem Zertifikat, das Sie löschen möchten.
3. Klicken Sie auf **Delete**, und bestätigen Sie, dass Sie das Zertifikat löschen möchten.

Anzeigen von Details des Zertifikats der vertrauten Serverzertifizierungsstelle

Sie können für jedes der auf dem IVE installierten Zertifizierungsstellenzertifikate eine Reihe von Details anzeigen.

So zeigen Sie Details des Zertifikats der vertrauten Serverzertifizierungsstelle an:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Trusted Server CAs**.

2. Klicken Sie auf das Zertifikat, das Sie anzeigen möchten.

3. Verwenden Sie unter **Certificate** den Pfeil neben den folgenden Feldnamen, um Zertifikatdetails anzuzeigen:

   - **Issued To** – Name und Attribute der Einheit, für die das Zertifikat ausgestellt ist.

   - **Issued By** – Name und Attribute der Einheit, die das Zertifikat ausgestellt hat. Beachten Sie, dass der Wert dieses Feldes entweder dem Inhalt des Feldes **Issued To** (für Stammzertifikate) oder dem des Feldes **Issued To** des nächsten Zertifikats weiter oben in der Kette (für Zwischenzertifikate) entsprechen sollte.

   - **Valid Dates** – Gültigkeitszeitraum des Zertifikats. Wenn Ihr Zertifikat abgelaufen ist, finden Sie diesbezügliche Anweisungen unter „Importieren eines erneuerten Zertifikats, das den vorhandenen privaten Schlüssel verwendet“ auf Seite 168.

   - **Details** – Beinhaltet verschiedene Zertifikatdetails, darunter Version, Seriennummer, Signaturalgorithmus, CRL-Verteilungspunkte, den öffentlichen Schlüssel und dessen Algorithmustyp. (Das IVE unterstützt nicht die CRL-Prüfung für Zertifikate vertrauter Serverzertifizierungsstellen.)

Registerkarte „Code-Signing Certificates“

Auf der Registerkarte **System > Configuration > Certificates > Code-Signing Certificates** können Sie wie unter „Codesignaturzertifikate“ auf Seite 72 beschrieben Codesignaturzertifikate für Benutzer importieren.

Importieren eines Codesignaturzertifikats

So importieren Sie ein Codesignaturzertifikat

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Code-Signing Certificates** aus.

2. Klicken Sie unter **Applet Signing Certificates** auf **Import Certificates**.

3. Wechseln Sie auf der Seite **Import Certificates** zu den entsprechenden Dateien mit dem Codesignaturzertifikat, geben Sie die Informationen für den Kennwortschlüssel ein, und klicken Sie dann auf **Import**.

4. Wenn Sie ein Zertifikat erfolgreich importiert haben, wird ein Dialogfeld **Sign Juniper Web Controls With** angezeigt, in dem Sie die Signaturoptionen des IVE festlegen können:

- **Default Juniper Certificate** – Wählen Sie diese Option aus, wenn das IVE alle vom IVE stammenden Active X- und Java-Applets mit dem Juniper Networks-Standardzertifikat signieren soll. Wenn Sie zuvor ein importiertes Codesignaturzertifikat ausgewählt haben und diese Option nach dem Klicken auf **Save** wiederherstellen, wird ein Prozesssymbol angezeigt. Dieses Symbol besagt, dass das IVE die Anfrage verarbeitet und den gesamten relevanten Code erneut signiert. Dieser Prozess kann einige Minuten in Anspruch nehmen.

- **Imported Certificate** – Wählen Sie diese Option aus, wenn das IVE alle Active X- und Java-Applets mit den in Schritt 3 importierten Zertifikaten signieren soll. Wenn Sie auf **Save** klicken, wird ein Prozesssymbol angezeigt. Dieses Symbol besagt, dass das IVE die Anfrage verarbeitet und den gesamten relevanten Code signiert. Dieser Prozess kann einige Minuten in Anspruch nehmen.

5. Legen Sie mit den Einstellungen auf den folgenden Registerkarten fest, welche Ressourcen vom Appletzertifikat signiert oder erneut signiert werden:

   - **Resource Policies > Web > Java > Code Signing** (siehe „Registerkarte „Code Signing““ auf Seite 317)

   - **Resource Policies > Web > Java > Applets** (siehe „Applets“ auf Seite 319)

Registerkarte „NCP“

Das Instant Virtual Extranet verwendet die folgenden Typen von internen Protokollen, um zwischen den Server- und Clientanwendungen des IVE zu kommunizieren:

- **Network Communications Protocol (NCP)** – Das IVE verwendet NCP zur Kommunikation mit Network Connect über SSL.

- **Optimized NCP (oNCP)** – Optimiertes NCP (oNCP) steigert die Durchsatzleistung der Clientanwendungen über NCP erheblich, da es die Protokolleffizienz, Verbindungsverarbeitung und Datenkomprimierung verbessert.

Festlegen von NCP-Optionen für Remoteclients

So legen Sie NCP-Optionen fest:

1. Wählen Sie in der Webkonsole, die Optionen **System > Configuration > NCP** aus.

2. Wählen Sie unter **NCP Auto-Select** Folgendes aus:

   - **Auto-select Enabled** (empfohlen) oNCP wird standardmäßig verwendet. Bei Auswahl dieser Option verwendet das IVE oNCP für den Großteil der Client-/Server-Kommunikation und wechselt dann ggf. zu Standard-NCP. Das IVE wechselt zurück zu NCP, wenn der Benutzer ein nicht unterstütztes Betriebssystem, einen nicht unterstützten Browsertyp oder eine Kombination dieser beiden Möglichkeiten verwendet oder wenn die Clientanwendung keine direkte TCP-Verbindung mit dem IVE herstellen kann (z. B. bei Vorhandensein eines Proxys, einer Zeitüberschreitung oder einer Verbindungstrennung).

   - **Auto-select Disabled** Es wird immer Standard-NCP verwendet. Diese Option wird in erster Linie aus Gründen der Abwärtskompatibilität bereitgestellt.

HINWEIS: Wenn Sie Network Connect für den Clientzugriff verwenden, ist bei der Verwendung der Option **Auto-select Disabled** Vorsicht geboten, da Mac- und Linux-Clients mit dem herkömmlichen NCP-Protokoll keine Verbindung herstellen können. Wenn Sie die automatische oNCP/NCP-Auswahlfunktion deaktivieren und ein UDP-zu-oNCP/NCP-Failover stattfindet, trennt das IVE die Verbindung von Macintosh- und Linux-Clients, da es von UDP zu NCP wechselt (anstelle von oNCP) und dieses Protokoll diese Benutzer nicht unterstützt.

3. (Java-Clients) Legen Sie unter **Read Connection Timeout** das Zeitlimit für Java-Clients (15-120 Sekunden) fest. Wenn clientseitige Secure Access-Methoden vom IVE keine Daten für das angegebene Intervall erhalten, wird versucht, erneut eine Verbindung mit dem IVE herzustellen. Beachten Sie, dass sich dieser Wert nicht auf Benutzerinaktivität in Clientanwendungen bezieht.

4. (Windows-Clients) Legen Sie unter **Idle Connection Timeout** das Intervall für das Leerlaufzeitlimit fest. Dieses Leerlaufintervall bestimmt, wie lange das IVE Verbindungen im Leerlauf für clientseitige Secure Access-Methoden für Windows aufrecht erhält.

5. Klicken Sie auf **Save Changes**.

Registerkarte „Client Types“

Auf der Registerkarte **Client Types** können Sie die Systemtypen, von denen sich Benutzer anmelden können, und die bei ihrer Anmeldung vom IVE angezeigten HTML-Seiten bestimmen.

Verwalten von Benutzer-Agents

So verwalten Sie Benutzer-Agents:

1. Wählen Sie in der Webkonsole, die Optionen **System > Configuration > Client Types**.

2. Geben Sie die Benutzer-Agent-Zeichenfolge ein, die dem Betriebssystem oder den Betriebssystemen entspricht, das oder die Sie unterstützen möchten. Sie können Ihre Angabe beliebig weit oder eingeschränkt gestalten. Sie können z. B. die Standardeinstellung des IVE für ***DoCoMo*** verwenden, um sie auf alle DoCoMo-Betriebssysteme anzuwenden, oder Sie können eine Zeichenfolge wie **DoCoMo/1.0/P502i/c10** erstellen, um einen einzelnen Typ von DoCoMo-Betriebssystem anzugeben. Sie können in Ihrer Zeichenfolge die Platzhalter * und ? verwenden. Für Benutzer-Agent-Zeichenfolgen im IVE muss die Groß-/Kleinschreibung nicht beachtet werden.

3. Geben Sie an, welchen HTML-Typ das IVE Benutzern anzeigen soll, die sich von dem im vorherigen Schritt angegebenen Betriebssystem anmelden. Folgende Optionen stehen zur Verfügung:

   - **Standard HTML** – Das IVE zeigt alle HTML-Standardfunktionen an, einschließlich Tabellen, Bilder in voller Größe, JavaScript, ActiveX-Komponenten, Java, Frames und Cookies. Diese Option ist ideal für Standardbrowser wie Firefox, Mozilla und Internet Explorer.

   - **Mobile HTML** – Das IVE zeigt HTML-kompatible Seiten für kleine Bildschirme an, die Tabellen, kleine Grafiken, JavaScript, Frames und Cookies enthalten können. In diesem Modus können jedoch keine Java-Applets oder ActiveX-Komponenten angezeigt werden. Ideal für Pocket PC-Browser.

   - **Smart Phone HTML Advanced** – Das IVE zeigt HTML-kompatible Seiten für kleine Bildschirme an, die Tabellen, kleine Grafiken, Frames, Cookies und JavaScript enthalten können. In diesem Modus können jedoch keine Java-Applets, ActiveX-Komponenten oder VB-Skripts angezeigt werden. Diese Option ist ideal für Treo- und Blazer-Browser.

   - **Smart Phone HTML Basic** – Das IVE zeigt HTML-kompatible Seiten für kleine Bildschirme an. Dieser Modus unterstützt weder Cookies noch die Anzeige von Tabellen, Grafiken, ActiveX-Komponenten, JavaScript, Java, VB-Skript oder Frames. (Der einzige Unterschied zwischen dieser Option und der Option **Compact HTML** ist die Benutzeroberfläche.) Diese Option ist ideal für Opera-Browser unter Symbian.

   - **Compact HTML** – Das IVE zeigt HTML-kompatible Seiten für kleine Bildschirme an. Dieser Modus unterstützt weder Cookies noch die Anzeige von Tabellen, Grafiken, ActiveX-Komponenten, JavaScript, Java, VB-Skript oder Frames. (Der einzige Unterschied zwischen dieser Option und der Option **Smart Phone HTML Basic** ist die Benutzeroberfläche.) Diese Option ist ideal für iMode-Browser.

HINWEIS: Das IVE schreibt Hyperlinks neu und fügt in den URL die Sitzungs-ID ein, anstatt Cookies zu verwenden.

4. Geben Sie die Reihenfolge an, in der das IVE die Benutzer-Agents auswerten soll. Das IVE wendet die erste Regel in der Liste an, die dem System des Benutzers entspricht. Sie können beispielsweise die folgenden Zuordnungen zwischen Benutzer-Agent-Zeichenfolgen und HTML-Typ in dieser Reihenfolge erstellen:

a. Benutzer-Agent-Zeichenfolge: ***DoCoMo*** Entspricht: **Compact HTML**

b. Benutzer-Agent-Zeichenfolge: **DoCoMo/1.0/P502i/c10** Entspricht: **Mobile HTML**

Wenn sich ein Benutzer von den in der zweiten Zeile angegebenen Betriebssystem anmeldet, zeigt ihm das IVE Compact HTML-Seiten an, und nicht das sicherere HTML für Mobilgeräte, weil seine Benutzer-Agent-Zeichenfolge dem ersten Element in der Liste entspricht.

Aktivieren Sie zum Anordnen von Zuordnungen in der Liste das Kontrollkästchen neben einem Element, und verschieben Sie es dann mit den nach oben und unten zeigenden Pfeilen zur richtigen Position in der Liste.

5. Aktivieren Sie das Kontrollkästchen **Enable password masking for Compact HTML**, wenn Sie Kennwörter maskieren möchten, die mit iMode oder anderen Geräten eingegeben wurden, die Compact HTML verwenden. (Geräte, die kein Compact HTML verwenden, maskieren Kennwörter immer, unabhängig davon, ob Sie dieses Kontrollkästchen aktivieren oder nicht.) Wenn die Kennwörter Ihrer iMode-Benutzer nicht-numerische Zeichen enthalten, müssen Sie die Kennwortmaskierung deaktivieren, weil iMode-Geräte nur numerische Daten in Standardkennwortfeldern zulassen. Wenn Sie die Maskierung deaktivieren, werden Kennwörter weiterhin sicher übertragen, aber auf der Anzeige des Benutzers nicht verborgen.

6. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „Network“

Die Seite **Network** enthält die folgenden Registerkarten:

- „Registerkarte „Overview““ auf Seite 186 – Die Einstellungen auf dieser Registerkarte dienen zum Konfigurieren allgemeiner Netzwerkeinstellungen.
- „Registerkarten „Internal Port““ auf Seite 187 – Die Einstellungen auf diesen Registerkarten dienen zum Ändern von Netzwerkeinstellungen für den internen Port, Festlegen statischer Routen und Hinzufügen eines statischen Eintrags.
- „Registerkarten „External Port““ auf Seite 188 – Die Einstellungen auf diesen Registerkarten dienen zum Ändern von Netzwerkeinstellungen für den externen Port, Festlegen statischer Routen und Hinzufügen eines statischen Eintrags.
- „Registerkarte „Routes““ auf Seite 189 – Die Einstellungen auf dieser Registerkarte dienen zum Definieren statischer Routen.
- „Registerkarte „Hosts““ auf Seite 190 – Die Einstellungen auf dieser Registerkarte dienen zum Festlegen von Hostnamen zur lokalen Auflösung durch das IVE.
- „Registerkarte „Network Connect““ auf Seite 190 – Die Einstellungen auf dieser Registerkarte dienen zum Herunterladen des Network Connect-Installationsprogramms, Definieren von IP-Filtern für Network Connect-IP-Adresspools und Festlegen der Server-IP-Adresse für Network Connect.

Registerkarte „Overview“

Verwenden Sie die Einstellungen auf dieser Registerkarte wie unter „Konfigurieren allgemeiner Netzwerkeinstellungen“ auf Seite 123 beschrieben zum Konfigurieren allgemeiner Netzwerkeinstellungen.

Konfigurieren allgemeiner Netzwerkeinstellungen

So konfigurieren Sie allgemeine Netzwerkeinstellungen:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Overview** aus.
2. Geben Sie unter **Network Identity** den vollständig qualifizierten Hostnamen des IVE ein.

HINWEIS: Der in diesem Feld eingegebene Hostname kann maximal 30 Zeichen lang sein.

3. Aktualisieren Sie unter **DNS Name Resolution** die primäre DNS-Adresse, die sekundäre DNS-Adresse und den DNS-Standarddomänennamen für die IVE-Appliance.

Sie können eine durch Kommas getrennte Liste von DNS-Domänen in diese Felder eingeben. Das IVE durchsucht sie in der Reihenfolge, in der sie aufgelistet sind.

4. Führen Sie unter **Windows Networking** die folgenden Aufgaben aus:

   - Geben Sie den Namen oder die IP-Adresse eines lokalen oder Remote-WINS-Servers (Windows Internet Naming Service) ein, mit dem Sie Namen von Arbeitsstationen und Standorte zu IP-Adressen zuordnen (sofern zutreffend).

   - Klicken Sie auf **Master Browser(s)**, um einen WINS-Server, einen Domänencontroller oder einen anderen Server in der IVE-Domäne auszuwählen, der auf NETBIOS-Aufrufe reagiert und Namen von Arbeitsstationen und Standorte zu IP-Adressen zuordnet (sofern zutreffend). Fügen Sie den Masterbrowser über die Seite **Windows Networking – Specify Master Browser** hinzu.

5. Aktivieren Sie das Kontrollkästchen **Enable network discovery**, damit das IVE freigegebene Windows-Ordner erkennen kann.

6. Klicken Sie auf **Save Changes**.

Registerkarten „Internal Port“

Verwenden Sie die folgenden Unterregisterkarten **Internal Port**, um Netzwerkeinstellungen für den internen Port zu ändern:

- „Registerkarte „Einstellungen““ auf Seite 187
- „Registerkarte „ARP Cache““ auf Seite 188

HINWEIS: In den meisten Feldern dieser Seite werden die bei der IVE-Installation eingegebenen Einstellungen angezeigt.

Registerkarte „Einstellungen“

So ändern Sie Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle):

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Internal Port > Settings** aus.

2. Aktualisieren Sie im Abschnitt **Port Information** die Einstellungen für IP-Adresse, Netzmaske, Gateway und Übertragungsrate für die jeweilige IVE-Appliance. Diese Felder enthalten standardmäßig die Einstellungen, die beim ersten IVE-Setup eingegeben wurden.

3. Geben Sie im Feld **ARP Ping Timeout** an, wie lange das IVE höchstens auf Antworten auf ARP-Anforderungen (Address Resolution Protocol) warten soll.

4. Geben Sie im Feld **MTU** eine maximale Übertragungseinheit für die interne Schnittstelle des IVE an.

HINWEIS: Verwenden Sie die Standardeinstellung (1500), sofern Sie die Einstellung nicht zwecks Problembehandlung ändern müssen.

5. Klicken Sie auf **Save Changes**.

Registerkarte „ARP Cache“

Hinzufügen eines statischen Eintrags

So fügen Sie einen statischen Eintrag hinzu:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Internal Port > ARP Cache** aus.

2. Nehmen Sie im oberen Bereich der Tabelle in den dafür vorgesehenen Feldern **IP Address** und **Physical Address** die entsprechenden Eingaben vor.

HINWEIS: Wenn Sie einen Eintrag mit einer bereits vorhandenen IP-Adresse hinzufügen, überschreibt das IVE den vorhandenen Eintrag mit dem neuen Eintrag. Außerdem sollten Sie beachten, dass das IVE nicht die Gültigkeit von MAC-Adressen überprüft.

3. Klicken Sie auf **Add**.

Registerkarten „External Port“

Verwenden Sie die folgenden Unterregisterkarten **External Port**, um Netzwerkeinstellungen für den externen Port zu ändern:

- „Registerkarte „Einstellungen““ auf Seite 188
- „Registerkarte „ARP Cache““ auf Seite 189

Registerkarte „Einstellungen“

Aktivieren des externen Ports (DMZ-Schnittstelle)

So aktivieren Sie den externen Port

1. Wählen Sie in der Webkonsole die Optionen **System > Network > External Port > Settings** aus.

2. Aktivieren Sie unter **Use External Port** die Option **Enabled**.

3. Geben Sie im Abschnitt **Port Information** die IP-Adresse, Netzmaske, das Gateway und die Übertragungsrate für den externen Port des IVE ein. In der Regel empfiehlt es sich, die Einstellungen der Seite **Internal Port > Settings** zu übernehmen und dann die Informationen zum internen Port in eine lokale IP-Adresse und Netzmaske sowie ein lokales Gateway zu ändern.

4. Geben Sie im Feld **ARP Ping Timeout** an, wie lange das IVE höchstens auf Antworten auf ARP-Anforderungen (Address Resolution Protocol) warten soll.

5. Geben Sie im Feld **MTU** eine maximale Übertragungseinheit für die externe Schnittstelle des IVE an.

HINWEIS: Verwenden Sie die Standardeinstellung (1500), sofern Sie die Einstellung nicht zwecks Problembehandlung ändern müssen.

---

6. Klicken Sie auf **Save Changes**.

Registerkarte „ARP Cache“

Hinzufügen eines statischen Eintrags

So fügen Sie einen statischen Eintrag hinzu:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > External Port > ARP Cache** aus.

2. Nehmen Sie im oberen Bereich der Tabelle in den dafür vorgesehenen Feldern **IP Address** und **Physical Address** die entsprechenden Eingaben vor.

HINWEIS: Wenn Sie einen Eintrag mit einer bereits vorhandenen IP-Adresse hinzufügen, überschreibt das IVE den vorhandenen Eintrag mit dem neuen Eintrag. Außerdem sollten Sie beachten, dass das IVE nicht die Gültigkeit von MAC-Adressen überprüft.

---

3. Klicken Sie auf **Add**.

Registerkarte „Routes“

Angeben von statischen Routen für den Netzwerkverkehr

So geben Sie statische Routen an

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Routes** aus.

2. Wählen Sie im Dropdownmenü **View route table for** eine Zielroutentabelle aus.

3. Klicken Sie auf **New Route**.

4. Geben Sie die erforderlichen Informationen ein.

5. Klicken Sie auf **Add to [destination] route table**.

   Zielroutentabellen sind für „Internal“, „External“ oder bei Verwendung von VLANs für alle definierten VLANs verfügbar.

Registerkarte „Hosts“

Angeben von Hostnamen zur lokalen Auflösung durch das IVE

So geben Sie Hostnamen zur lokalen Auflösung durch das IVE an:

1. Wählen Sie in der Webkonsole die Registerkarte **System > Network > Hosts** aus.

2. Geben Sie eine IP-Adresse, eine durch Kommas getrennte Liste von Hostnamen, die zu der IP-Adresse aufgelöst werden, und bei Bedarf einen Kommentar von höchstens 200 Wörtern ein, und klicken Sie dann auf **Add**.

Registerkarte „Network Connect“

Auf der Registerkarte Network Connect können Sie IP-Filter für das IVE angeben, die auf Network Connect-IP-Pools angewendet werden sollen. Weitere Informationen finden Sie unter „Network Connect – Übersicht“ auf Seite 95.

Herunterladen des Network Connect-Installationsprogramms

Die Network Connect-Anwendung kann über die Seite **Maintenance > System > Installers** als ausführbare Windows-Datei heruntergeladen werden. Weitere Informationen finden Sie unter „Herunterladen von Anwendungen oder Diensten“ auf Seite 362.

Angeben von IP-Filtern, die auf Network Connect-IP-Pools angewendet werden sollen

So fügen Sie der Network Connect-Filterliste eine IP-Adresse hinzu:

1. Wählen Sie in der Webkonsole, die Optionen **System > Network > Network Connect** aus.

2. Geben Sie eine Kombination aus IP-Adresse und Netzmaske an, und klicken Sie dann auf **Add**. Das IVE wendet die auf dieser Seite angegebenen Filter auf die Ressourcenrichtlinien für Network Connect-IP-Pools an, die auf eine Anforderung eines Benutzers angewendet werden.

Angeben der IP-Adresse für Network Connect Server

Der serverseitige Network Connect-Prozess verwendet die IP-Adresse für die Kommunikation mit Unternehmensressourcen. Obwohl das IVE dieses Feld vorab ausfüllt, können Sie die Adresse bei Bedarf ändern, sofern sie keinem in einem NC-Verbindungsprofil festgelegten IP-Adresspool angehört (siehe „Erstellen eines Network Connect-Verbindungsprofils“ auf Seite 347).

Konfigurieren der Seite „Log Monitoring“

Die Seite **Log Monitoring** enthält die folgenden Registerkarten:

- „Registerkarten „Events“, „User Access“ „Admin Access“ und „NC Packet““ auf Seite 191 – Verwenden Sie diese Registerkarten zum Speichern von Protokolldateien und Festlegen der in den Protokolldateien zu speichernden Ereignisse.
- „Registerkarte „SNMP““ auf Seite 193 – Verwenden Sie diese Registerkarte zum Überwachen des IVE als SNMP-Agent.
- „Registerkarte „Statistics““ auf Seite 199 – Verwenden Sie diese Registerkarte zum Anzeigen von Systemstatistiken.
- „Registerkarte „Client-side Logs““ auf Seite 199 – Diese Registerkarte dient zum Aktivieren clientseitiger Protokolle für Host Checker, Cache Cleaner und Network Connect-Funktionen.

Weitere Informationen zu Protokollen und Überwachungsfunktionen des IVE finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 126.

Registerkarten „Events“, „User Access“ „Admin Access“ und „NC Packet“

Auf den Seiten **System > Log/Monitoring > Events**, **User Access**, **Admin Access** und **NC Packet** können Sie Protokolldateien speichern, dynamische Protokollabfragen erstellen, die in den Protokolldateien zu speichernden Dateien festlegen und benutzerdefinierte Filter und Formate erstellen.

Die Seiten **Events Log**, **User Access Log**, **Admin Access Log** und **NC Packet Log** enthalten die folgenden Registerkarten:

- „Registerkarte „Log““ auf Seite 191
- „Registerkarte „Einstellungen““ auf Seite 192

HINWEIS: Bei den Ereignis-, Benutzerzugriffs- und Administratorzugriffsprotokollen handelt es sich um drei eigenständige Dateien. Obwohl die grundlegenden Konfigurationsanweisungen für alle drei gleich sind, wirken sich Einstellungsänderungen bei einer der Dateien nicht auf die Einstellungen der anderen aus. Weitere Informationen zu den Inhalten der einzelnen Dateien finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 126.

Registerkarte „Log“

Speichern, Anzeigen oder Löschen der Protokolldatei

So zeigen Sie die Ereignisprotokolldatei an, speichern sie oder löschen sie:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring** aus.

2. Öffnen Sie die Registerkarte **Events Log**, **User Access Log**, **Admin Access Log** oder **NC Packet Log**, und klicken Sie dann auf **Log**.

3. Geben Sie im Feld **Show** eine Zahl ein, und klicken Sie auf **Update**, wenn Sie die Anzahl der jeweils vom IVE angezeigten Protokolleinträge ändern möchten.

4. Klicken Sie auf **Save Log As**, wechseln Sie zum gewünschten Netzwerkspeicherort, geben Sie einen Dateinamen ein, und klicken Sie dann auf **Save**, um die Protokolldatei manuell zu speichern.

5. Klicken Sie auf **Clear Log**, um das lokale Protokoll und die Datei log.old zu löschen.

HINWEIS: Wenn Sie das lokale Protokoll löschen, wirkt sich dies nicht auf die vom Syslog-Server aufgezeichneten Ereignisse aus. Die nachfolgenden Ereignisse werden in einer neuen lokalen Protokolldatei aufgezeichnet.

Registerkarte „Einstellungen“

Geben Sie an, welche Ereignisse in der Protokolldatei gespeichert werden sollen.

Mithilfe der Optionen auf der Registerkarte **Settings** können Sie neben der Höchstdateigröße angeben, was das IVE in die Protokolldatei schreiben und welcher Syslog-Server zum Speichern der Protokolldateien verwendet werden soll.

HINWEIS: Sie können auch die Seite **Archiving** verwenden, um die Protokolle automatisch an einem für FTP zugänglichen Ort zu speichern. Weitere Informationen finden Sie unter „Konfigurieren der Seite „Archiving““ auf Seite 376.

So legen Sie die Einstellungen für das Ereignisprotokoll fest:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring** aus.

2. Öffnen Sie die Registerkarte **Events Log**, **User Access Log**, **Admin Access Log** oder **NC Packet Log**, und klicken Sie dann auf **Settings**.

3. Geben Sie im Feld **Maximum Log Size** die maximale Dateigröße für die lokale Protokolldatei an. (Die Grenze liegt bei 500 MB.) Im Systemprotokoll werden Daten bis zu der angegebenen Menge angezeigt.

4. Aktivieren Sie unter **Select Events to Log** die Kontrollkästchen für die einzelnen Ereignisarten, die in der lokalen Protokolldatei erfasst werden sollen.

HINWEIS: Wenn Sie das Kontrollkästchen **Statistics** auf der Registerkarte **Events Log** deaktivieren, schreibt das IVE die Statistiken nicht in die Protokolldatei, sondern es zeigt sie weiterhin auf der Registerkarte **System > Log/Monitoring > Statistics** an. Weitere Informationen finden Sie unter „Registerkarte „Statistics““ auf Seite 199.

HINWEIS: Der Bereich **Select Events to Log** der Registerkarte **Settings** gilt nicht für die Seite **NC Packet**, da bei der Network Connect-Paketprotokollierung nicht die verwaltungsorientierte Protokollierung im Mittelpunkt steht, sondern clientseitige Paketaktivitäten.

5. Geben Sie unter **Syslog Servers** Informationen über den Syslog-Server ein, auf dem die Protokolldateien gespeichert werden sollen (optional):

   a. Geben Sie den Namen oder die IP-Adresse des Syslog-Servers ein.

   b. Geben Sie einen Syslog-Typ („Facility“) für den Server ein. Das IVE stellt 8 Facilitys (LOCAL0-LOCAL7) bereit, die Sie den Facilitys auf dem Syslog-Server zuordnen können.

   c. Klicken Sie auf **Add**.

   d. Wiederholen Sie den Vorgang ggf. für mehrere Server, und verwenden Sie unterschiedliche Formate und Filter für verschiedene Server und Facilitys.

HINWEIS: Vergewissern Sie sich, dass der Syslog-Server Nachrichten mit den folgenden Einstellungen akzeptiert: facility = LOG_USER und level = LOG_INFO.

6. Klicken Sie auf **Save Changes**.

Registerkarte „SNMP“

Überwachen des IVE als SNMP-Agent

Über diese Registerkarte können Sie ein Netzwerkverwaltungstool wie HP OpenView zum Überwachen des IVE als SNMP-Agent verwenden. Das IVE unterstützt SNMP (Simple Network Management Protocol), Version 2, implementiert eine private MIB (Management Information Base) und definiert eigene Traps. Um die Verarbeitung dieser Traps in der Netzwerkverwaltungsstation zu ermöglichen, müssen Sie die Juniper Networks-MIB-Datei herunterladen und die entsprechenden Angaben zum Empfangen der Traps machen.

HINWEIS: Zum Überwachen wesentlicher IVE-Systemstatistiken, beispielsweise der CPU-Auslastung, laden Sie die UC-Davis-MIB-Datei in Ihre SNMP-Managementanwendung. Sie erhalten die MIB-Datei im Internet unter folgender Adresse: http://net-snmp.sourceforge.net/docs/mibs/UCD-SNMP-MIB.txt.

So legen Sie SNMP-Einstellungen fest

1. Wählen Sie in der Webkonsole **System > Log/Monitoring > SNMP** aus.

2. Klicken Sie auf die Verknüpfung **Juniper Networks MIB file**, um auf die MIB-Datei zuzugreifen, und speichern Sie die Datei dann im Browser an einem Netzwerkspeicherort. Beschreibungen der Get- und Trap-Objekte in der MIB-Datei finden Sie unter „Konfigurationsobjekte“ auf Seite 195 und „Status-/Fehlerobjekte“ auf Seite 197.

3. Geben Sie unter **Agent Properties** Informationen in die folgenden Felder ein, und klicken Sie anschließend auf **Save Changes**:

   - Geben Sie in die Felder **System Name**, **System Location** und **System Contact** Informationen ein, die den IVE-Agent beschreiben (optional).
   - Geben Sie im Feld **Community** eine Zeichenfolge ein (erforderlich).

HINWEIS: Zum Abfragen des IVEs muss Ihre Netzwerkverwaltungsstation diese Zeichenfolge an das IVE senden.

HINWEIS: Um das SNMP-System zu beenden, löschen Sie die Angaben im Feld **Community**.

4. Legen Sie unter **Trap Thresholds** die Werte für die folgenden Traps fest (optional):

   - **Check Frequency**
   - **Log Capacity**
   - **Users**
   - **Memory**
   - **Swap Memory**
   - **Disk**
   - **Meeting Users**
   - **CPU**

   Informationen zu Trap-Grenzwerten finden Sie unter „Konfigurationsobjekte“ auf Seite 195 und „Status-/Fehlerobjekte“ auf Seite 197.

5. Wählen Sie unter **Optional traps** folgende Optionen aus (optional):

   - **Critical Log Events**
   - **Major Log Events**

   Weitere Informationen zu diesen Ereignistypen finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 126.

6. Legen Sie unter **SNMP Servers** die Server fest, an die das IVE Traps senden soll, die es bei Eingabe von Daten in die folgenden Felder generiert, und klicken Sie anschließend auf **Add**:

   - Der Hostname oder die IP-Adresse des Servers
   - Der Port, an dem der Server Daten abfragt (üblicherweise Port 162)

- Die von der Netzwerkverwaltungsstation benötigte Community-Zeichenfolge (sofern vorhanden)

7. Klicken Sie auf **Save Changes**.

8. Gehen Sie in der Netzwerkverwaltungsstation folgendermaßen vor:

   a. Laden Sie die Juniper Networks-MIB-Datei herunter.

   b. Geben Sie die Community-Zeichenfolge an, die beim Abfragen des IVE benötigt wird (siehe Schritt 3).

   c. Konfigurieren Sie die Netzwerkverwaltungssoftware für den Empfang von IVE-Traps.

Tabelle 4: Konfigurationsobjekte

Objekt	Beschreibung
logFullPercent	Gibt den Prozentsatz der verfügbaren Dateigröße, der durch das aktuelle Protokoll belegt wird, als einen Parameter des logNearlyFull-Trap zurück.
signedInWebUsers	Gibt die Anzahl der über einen Webbrowser am IVE angemeldeten Benutzer zurück.
signedInMailUsers	Gibt die Anzahl der am E-Mail-Client angemeldeten Benutzer zurück.
blockedIP	Gibt die IP-Adresse zurück, die durch wiederholt fehlgeschlagene Anmeldeversuche blockiert ist und von der iveToomanyFailedLoginAttempts-Trap gesendet wurde. Das System fügt die blockierte IP-Adresse der Tabelle blockedIPList hinzu.
authServerName	Gibt den Namen des externen Authentifizierungsservers zurück, der von der externalAuthServerUnreachable-Trap gesendet wurde.
productName	Gibt den Produktnamen des lizenzierten IVE zurück.
productVersion	Gibt die Softwareversion des IVE-Systems zurück.
fileName	Gibt den Dateinamen zurück, der von der archiveFileTransferFailed-Trap gesendet wurde.
meetingUserCount	Gibt die Anzahl der gleichzeitig an der Konferenz angemeldeten Benutzer zurück, die von der meetingUserLimit-Trap gesendet wurde.
iveCpuUtil	Gibt den Prozentsatz der CPU-Auslastung während des Intervalls zwischen zwei SNMP-Abfragen zurück. Dieser Wert wird berechnet, indem die CPU-Auslastung durch die verfügbare CPU-Kapazität während der aktuellen und vorherigen SNMP-Abfragen geteilt wird. Ist keine vorherige Abfrage verfügbar, basiert die Berechnung auf dem Intervall zwischen der aktuellen Abfrage und dem Systemstart.
iveMemoryUtil	Gibt den Prozentsatz der Speicherauslastung des IVE während einer SNMP-Abfrage zurück. Dieser Wert wird berechnet, indem die Anzahl verwendeter Speicherseiten durch die Anzahl der verfügbaren Speicherseiten geteilt wird.

Tabelle 4: Konfigurationsobjekte (Fortsetzung)

Objekt	Beschreibung
iveConcurrentUsers	Gibt die Gesamtzahl von Benutzern zurück, die für den IVE-Knoten angemeldet sind.
clusterConcurrentUsers	Gibt die Gesamtzahl an Benutzern zurück, die am Cluster angemeldet sind.
iveTotalHits	Gibt die Gesamtzahl der Zugriffe auf das IVE seit dem letzten Neustart zurück.
iveFileHits	Gibt die Gesamtzahl der Dateizugriffe auf das IVE seit dem letzten Neustart zurück.
iveWebHits	Gibt die Gesamtzahl der Zugriffe über die Weboberfläche seit dem letzten Neustart zurück.
iveAppletHits	Gibt die Gesamtzahl der Appletzugriffe auf das IVE seit dem letzten Neustart zurück.
ivetermHits	Gibt die Gesamtzahl der Terminalzugriffe auf das IVE seit dem letzten Neustart zurück.
iveSAMHits	Gibt die Gesamtzahl der Secure Application Manager-Zugriffe auf das IVE seit dem letzten Neustart zurück.
iveNCHits	Gibt die Gesamtzahl der Network Connect-Zugriffe auf das IVE seit dem letzten Neustart zurück.
meetingHits	Gibt die Gesamtzahl der Konferenzzugriffe auf das IVE seit dem letzten Neustart zurück.
meetingCount	Gibt die Anzahl der gleichzeitig stattfindenden Konferenzen zurück, die von der meetingLimit-Trap gesendet wurde.
logName	Gibt den Namen des Protokolls (admin/user/event) für die logNearlyFull- und iveLogFull-Trap zurück.
iveSwapUtil	Gibt den Prozentsatz der vom IVE während einer SNMP-Abfrage verwendeten Auslagerungsspeicherseiten zurück. Dieser Wert wird berechnet, indem die Anzahl verwendeter Auslagerungsspeicherseiten durch die Anzahl der verfügbaren Auslagerungsspeicherseiten geteilt wird.
diskFullPercent	Gibt den Prozentsatz des vom IVE genutzten Festplattenspeichers für die iveDiskNearlyFull-Trap zurück. Dieser Wert wird berechnet, indem die Anzahl der verwendeten Speicherblöcke durch die Gesamtzahl der Speicherblöcke geteilt wird.
blockedIPList	Gibt eine Tabelle mit den 10 zuletzt blockierten IP-Adressen zurück. Die blockedIP-MIB fügt dieser Tabelle blockierte IP-Adressen hinzu.
ipEntry	Ein Eintrag in der Tabelle blockedListIP mit einer blockierten IP-Adresse und ihrem Index (siehe IPEntry).
IPEntry	Der Index (ipIndex) und die IP-Adresse (ipValue) für einen Eintrag in der Tabelle blockedIPList.
ipIndex	Gibt den Index für die Tabelle blockedIPList zurück.
ipValue	Der Eintrag einer blockierten IP-Adresse in der Tabelle blockedIPList.
logID	Gibt die eindeutige ID der Protokollmeldung zurück, die von der logMessageTrap-Trap gesendet wurde.

Tabelle 4: Konfigurationsobjekte (Fortsetzung)

Objekt	Beschreibung
logType	Gibt eine vom logMessageTrap-Trap gesendete Zeichenfolge zurück, die besagt, dass eine Protokollmeldung wichtig oder kritisch ist.
logDescription	Gibt eine vom logMessageTrap-Trap gesendete Zeichenfolge zurück, die besagt, dass eine Protokollmeldung wichtig oder kritisch ist.

Tabelle 5: Status-/Fehlerobjekte

Objekt	Beschreibung
iveLogNearlyFull	Die durch den logName-Parameter festgelegte Protokolldatei (System, Benutzerzugriff oder Administratorzugriff) ist fast voll. Wenn dieses Trap gesendet wird, wird auch der Parameter logFullPercent (Protokolldatei ist zu % voll) gesendet. Für diese Trap kann ein beliebiger Prozentsatz konfiguriert werden. Setzen Sie iveLogNearlyFull zum Deaktivieren der Trap auf 0 %. Der Standardwert der Trap ist 90 %.
iveLogFull	Die Protokolldatei (System, Benutzerzugriff oder Administratorzugriff), die durch den logName-Parameter festgelegt wird, ist zu 100 % voll.
iveMaxConcurrentUsersSignedIn	Die definierte maximale Anzahl von Benutzern oder die zulässige Anzahl gleichzeitiger Benutzer ist zurzeit angemeldet. Für diese Trap kann ein beliebiger Prozentsatz konfiguriert werden. Setzen Sie iveMaxConcurrentUsersSignedIn zum Deaktivieren der Trap auf 0 %. Der Standardwert der Trap ist 100 %.
iveTooManyFailedLoginAttempts	Ein Benutzer mit einer bestimmten IP-Adresse hat zu viele fehlgeschlagene Anmeldeversuche unternommen. Diese Trap wird ausgelöst, wenn sich ein Benutzer nicht entsprechend den Einstellungen für die **Lockout Options** auf der Registerkarte **Security Options** authentifiziert. (Siehe „Konfigurieren von Sperroptionen“ auf Seite 165.) Wenn das System diese Trap auslöst, löst es auch den Parameter blockedIP aus (Quell-IP der Anmeldeversuche).
externalAuthServerUnreachable	Ein externer Authentifizierungsserver beantwortet keine Authentifizierungsanforderungen. Wenn diese Trap gesendet wird, wird auch der Parameter authServerName (% der Protokolldatei belegt)(Name des nicht erreichbaren Servers) gesendet.
iveStart	Das IVE wurde soeben eingeschaltet.
iveShutdown	Das IVE wurde soeben heruntergefahren.
iveReboot	Das IVE wurde soeben neu gestartet.
archiveServerUnreachable	Das IVE kann den konfigurierten FTP- oder SCP-Archivierungsserver nicht erreichen.
archiveServerLoginFailed	Das IVE kann sich nicht am konfigurierten FTP- oder SCP-Archivierungsserver anmelden.

Tabelle 5: Status-/Fehlerobjekte (Fortsetzung)

Objekt	Beschreibung
archiveFileTransferFailed	Das IVE kann keine erfolgreiche Übertragung des Archivs auf den konfigurierten FTP- oder SCP-Archivierungsserver ausführen. Wenn das System diese Trap sendet, sendet es auch den Parameter fileName.
meetingUserLimit	Sendet eine Benachrichtigung, dass die Anzahl der Benutzer über dem Lizenzlimit liegt. Wenn das System diese Trap sendet, sendet es auch den Parameter meetingUserCount.
iveRestart	Sendet eine Benachrichtigung, dass das IVE gemäß den Anweisungen des Administrators neu gestartet wurde.
meetingLimit	Sendet eine Benachrichtigung, dass die Anzahl an gleichzeitigen Konferenzen über dem Lizenzlimit liegt. Wenn das System diese Trap sendet, sendet es auch den Parameter meetingCount. Für diese Trap kann ein beliebiger Prozentsatz konfiguriert werden. Setzen Sie meetingLimit zum Deaktivieren der Trap auf 0%. Der Standardwert der Trap ist 100%.
iveDiskNearlyFull	Sendet eine Benachrichtigung, dass die Festplatte des IVE nahezu voll ist. Wenn das System diese Trap sendet, sendet es auch den Parameter diskFullPercent. Für diese Trap kann ein beliebiger Prozentsatz konfiguriert werden. Setzen Sie iveDiskNearlyFull zum Deaktivieren der Trap auf 0%. Der Standardwert der Trap ist 80%.
iveDiskFull	Sendet eine Benachrichtigung, dass die Festplatte des IVE voll ist.
logMessageTrap	Die aus einer Protokollmeldung generierte Trap. Wenn das System diese Trap sendet, sendet es auch die Parameter logID, logType und logDescription.
memUtilNotify	Sendet eine Benachrichtigung, dass das System den konfigurierten Grenzwert für die Arbeitsspeicherauslastung erreicht hat. Setzen Sie memUtilNotify zum Deaktivieren der Trap auf 0. Der Standardgrenzwert ist 0%.
cpuUtilNotify	Sendet eine Benachrichtigung, dass das System den konfigurierten Grenzwert für die CPU-Auslastung erreicht hat. Setzen Sie cpuUtilNotify zum Deaktivieren der Trap auf 0. Der Standardgrenzwert ist 0%.
swapUtilNotify	Sendet eine Benachrichtigung, dass das System den konfigurierten Grenzwert für die Auslagerungsspeicherauslastung erreicht hat. Setzen Sie swapUtilNotify zum Deaktivieren der Trap auf 0. Der Standardgrenzwert ist 0%.

Registerkarte „Statistics“

Anzeigen der Systemstatistik

Die Seite **Statistics** zeigt die Anzahl der angemeldeten Benutzer der letzten sieben Tage an. Diese Informationen werden einmal wöchentlich in das Systemprotokoll geschrieben. Beim Aktualisieren des IVE werden alle Statistiken gelöscht. Wenn Sie das System so konfigurieren, dass es stündlich die Statistik protokolliert, sind die alten Statistiken nach einer Aktualisierung immer noch in der Protokolldatei verfügbar.

So zeigen Sie die Systemstatistik an:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring > Statistics** aus.
2. Führen Sie auf der Seite einen Bildlauf durch, um alle Daten anzuzeigen.

Registerkarte „Client-side Logs“

Auf der Registerkarte **System > Log/Monitoring > Client-side Log** können Sie die clientseitige Protokollierung für die Funktionen von Host Checker, Cache Cleanerund Network Connect aktivieren. Wenn Sie diese Option für eine Funktion aktivieren, schreibt das IVE ein clientseitiges Protokoll für jeden Client, der diese Funktion verwendet. Bei jedem Aufruf dieser Funktion in nachfolgenden Benutzersitzungen fügt das IVE Informationen zur Protokolldatei hinzu. Diese Funktion ist bei der Zusammenarbeit mit dem Support-Team nützlich, um mit der entsprechenden Funktion zusammenhängende Probleme zu debuggen.

HINWEIS:

- Da diese Einstellungen global sind, schreibt das IVE eine Protokolldatei für alle Clients, die die Funktion verwenden, für die Sie die clientseitige Protokollierung aktivieren. Außerdem entfernt das IVE keine clientseitigen Protokolle. Benutzer müssen Protokolldateien manuell von ihren Clients löschen. Weitere Informationen darüber, wo das IVE Protokolldateien installiert, finden Sie unter „Installation von clientseitigen Anwendungen“ auf Seite 411.
- Wenn Network Connect-Benutzer die clientseitige Protokollierung deaktivieren (auch wenn die Protokollierung anhand des folgenden Verfahrens auf dem IVE aktiviert wird), zeichnet der Client keine clientseitigen Protokollinformationen auf. Wenn der Benutzer die Protokollierungsfunktion aktiviert und das IVE dann zum Deaktivieren der clientseitigen Protokollierung konfiguriert wird, zeichnet der Client keine neuen clientseitigen Protokollinformationen auf.

Festlegen von Einstellungen für clientseitige Protokollierung

So legen Sie Einstellungen für clientseitige Protokollierung fest:

1. Wählen Sie in der Webkonsole, die Optionen **System > Log/Monitoring > Client-side Log**.

2. Wählen Sie die gewünschten Funktionen aus, für die das IVE clientseitige Protokolle schreibt.

3. Klicken Sie zum globalen Speichern der Einstellungen auf **Save Changes**.

HINWEIS: Für neue Systeme sind alle Optionen standardmäßig *deaktiviert*.

Kapitel 7

Anmeldeeinstellungen

Mit den Einstellungen im Abschnitt **Signing In** der Webkonsole können Anmelderichtlinien und -seiten sowie Endpunktüberprüfungsoptionen konfiguriert und Authentifizierungsserver eingerichtet werden.

Inhalt

- „Konfigurieren der Seite „Sign-in““ auf Seite 203
- „Konfigurieren der Seite „End Point““ auf Seite 206
- „Konfigurieren der Seite „AAA Servers““ auf Seite 223

Konfigurieren der Seite „Sign-in“

Die Seite **Sign-in** enthält die folgenden Registerkarten:

- „Registerkarte „Sign-in Policies““ auf Seite 203 – Diese Registerkarte dient zum Erstellen und Konfigurieren von Anmelderichtlinien.
- „Registerkarte „Sign-in Pages““ auf Seite 204 – Diese Registerkarte dient zum Erstellen oder Ändern einer Standardanmeldeseite.

Registerkarte „Sign-in Policies“

Diese Registerkarte dient zum Erstellen und Konfigurieren von Anmelderichtlinien. *Anmelderichtlinien* definieren wie unter „Anmelderichtlinien – Übersicht“ auf Seite 55 beschrieben die URLs, die Benutzer und Administratoren für den Zugriff auf das IVE verwenden können.

Konfigurieren von Administrator- und Benutzeranmelderichtlinien

So konfigurieren Sie Administrator- und Benutzeranmelderichtlinien:

1. Wählen Sie in der Webkonsole die Optionen **Signing In > Sign-in > Sign-in Policies** aus.
2. Klicken Sie in der Spalte **Administrator URLs** bzw. **User URLs** auf den URL.
3. Ändern Sie den zugeordneten URL dieser Richtlinie (optional).
4. Geben Sie unter **Description** eine Beschreibung für die Richtlinie ein (optional).
5. Wählen Sie unter **Sign-in Page** eine Anmeldeseite aus. Sie können die Standardseite für das IVE oder eine Variation der Standardanmeldeseite auswählen. Weitere Informationen finden Sie unter „Registerkarte „Sign-in Pages““ auf Seite 204.
6. Legen Sie unter **Authentication realm** fest, welche Bereiche der Richtlinie zugeordnet werden sollen und wie Benutzer und Administratoren Bereiche auswählen sollen. Wenn Sie Folgendes auswählen:
   - **User types the realm name** – Das IVE ordnet die Anmelderichtlinie allen Authentifizierungsbereichen zu, es zeigt jedoch keine Bereichsliste an, in der der Benutzer oder Administrator eine Auswahl treffen kann. Stattdessen muss der Benutzer oder Administrator seinen Bereichsnamen manuell auf der Anmeldeseite eingeben.

- **User picks from a list of authentication realms** – Das IVE ordnet die Anmelderichtlinie nur den ausgewählten Authentifizierungsbereichen zu. Das IVE zeigt dem Benutzer oder Administrator diese Bereichsliste bei der Anmeldung am IVE an und ermöglicht die Auswahl eines in der Liste aufgeführten Bereichs. (Wenn dem URL nur ein einziger Bereich zugeordnet ist, zeigt das IVE keine Dropdownliste von Bereichen an. Stattdessen verwendet es automatisch den von Ihnen festgelegten Bereich.)

HINWEIS: Wenn Sie dem Benutzer die Auswahl aus mehreren Bereichen erlauben und einer dieser Bereiche einen anonymen Authentifizierungsserver verwendet, zeigt das IVE diesen Bereich nicht in der Dropdownliste mit den Bereichen an. Um die Anmelderichtlinie effektiv einem anonymen Bereich zuzuordnen, müssen Sie diesen Bereich nur der Liste **Authentication realm** hinzufügen.

7. Klicken Sie auf **Save Changes**.

Aktivieren und Deaktivieren von Anmelderichtlinien

So aktivieren und deaktivieren Sie Anmelderichtlinien:

1. Wählen Sie in der Webkonsole die Optionen **Signing In > Sign-in > Sign-in Policies** aus.
2. So gehen Sie für die Aktivierung oder Deaktivierung vor:
   - **Einzelne Richtlinie** – Aktivieren Sie das Kontrollkästchen neben der Richtlinie, die Sie ändern möchten, und klicken Sie dann auf **Enable** oder **Disable**.
   - **Alle Benutzer- und Konferenzrichtlinien** – Aktivieren oder deaktivieren Sie oben auf der Seite das Kontrollkästchen **Restrict access to administrators only**.

Registerkarte „Sign-in Pages“

Diese Registerkarte dient zum Erstellen oder Ändern einer Standardanmeldeseite. Eine *Anmeldeseite* legt wie unter „Anmeldeseiten“ auf Seite 55 beschrieben die benutzerdefinierten Eigenschaften der Willkommensseite des Benutzers fest, z. B. Begrüßungstext, Hilfetext, Logo, Kopf- und Fußbereich.

Erstellen oder Bearbeiten einer Standardanmeldeseite

So erstellen oder bearbeiten Sie eine Standardanmeldeseite:

1. Wählen Sie in der Webkonsole die Optionen **Signing In > Sign-in > Sign-in Pages** aus.
2. Gehen Sie dabei folgendermaßen vor:
   - **Erstellen einer neuen Seite** – Klicken Sie auf **New Page**.
   - **Bearbeiten einer vorhandenen Seite** – Wählen Sie die entsprechende Verknüpfung für die zu bearbeitende Seite aus.

3. Geben Sie einen Namen für die Seite ein.

4. Ändern Sie im Abschnitt **Custom text** den für die verschiedenen Fensterbeschriftungen verwendeten Standardtext nach Bedarf. Wenn Sie im Feld **Instructions** Text hinzufügen, ist zu beachten, dass das Formatieren von Text und Hinzufügen von Verknüpfungen anhand der folgenden HTML-Tags erfolgen kann: <i>, <b>, <br>, <font> und <a href>. Allerdings schreibt das IVE Verknüpfungen auf der Anmeldseite (aufgrund der noch nicht erfolgten Benutzerauthentifizierung) nicht neu. Folglich sollten Sie nur Verweise auf externe Sites erstellen. Verknüpfungen zu Sites hinter einer Firewall funktionieren nicht.

HINWEIS: Wenn Sie in der benutzerdefinierten Meldung nicht unterstützte HTML-Tags verwenden, zeigt das IVE die IVE-Startseite des Benutzers möglicherweise nicht korrekt an.

5. Legen Sie im Abschnitt **Header appearance** eine benutzerdefinierte Logobilddatei und eine andere Farbe für den Header fest.

6. Ändern Sie im Abschnitt **Custom error messages** den Standardtext, der im Fall von Zertifikatsfehler für Benutzer angezeigt wird.

7. Um Benutzern benutzerdefinierte Hilfeinformationen oder zusätzliche Anweisungen bereitzustellen, wählen Sie **Show Help Button** aus, geben Sie eine Beschriftung für die Schaltfläche ein, und geben Sie eine HTML-Datei an, die in das IVE hochgeladen werden soll. Beachten Sie, dass im IVE keine Bilder und anderen Inhalte angezeigt werden, auf die in dieser HTML-Seite verwiesen wird.

8. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, Benutzer mit aktiven Sitzungen müssen jedoch u. U. ihre Webbrowser aktualisieren.

HINWEIS: Klicken Sie auf **Restore Factory Defaults**, um die Darstellung der Anmeldeseite, der IVE-Benutzerstartseite und der Webkonsole zurückzusetzen.

Konfigurieren der Seite „End Point“

Die Seite **End Point** enthält die folgenden Registerkarten:

- „Registerkarte „Host Checker““ auf Seite 206 – Diese Registerkarte dient zum Festlegen von Host Checker-Optionen und Erstellen von Host Checker-Richtlinien.
- „Registerkarte „Cache Cleaner““ auf Seite 220 – Diese Registerkarte dient zum Festlegen von Cache Cleaner-Optionen.

Registerkarte „Host Checker“

Auf der Registerkarte **Signing In > End Point > Host Checker** können Sie allgemeine Host Checker-Optionen festlegen sowie globale clientseitige Richtlinien und globale serverseitige Richtlinien erstellen.

Festlegen von allgemeinen Host Checker-Optionen

Sie können globale Optionen für Host Checker festlegen, die auf alle Benutzer angewendet werden, für die gemäß einer Authentifizierungsrichtlinie oder einer Rollenzuordnungsregel Host Checker erforderlich ist.

So legen Sie allgemeine Host Checker-Optionen fest:

1. Wählen Sie in der Webkonsole **Signing In > End Point > Host Checker**.
2. Geben Sie unter **Options** Folgendes an:
   - Geben Sie im Feld **Perform check every X minutes** das Intervall an, in dem Host Checker auf einem Clientcomputer ausgeführt werden soll. Wenn der Clientcomputer die in einer Rolle definierten Anforderungen der Host Checker-Richtlinien nicht erfüllt, verweigert das IVE die entsprechenden Benutzeranfragen.

     Beispielsweise kann verlangt werden, dass ein Benutzer eine bestimmte Antivirenanwendung eines Drittanbieters ausführt, um Rolle A zugeordnet zu werden, wodurch Netzwerkverbindungen von einem externen Standort aktiviert werden. Wenn bei der Anmeldung des Benutzers beim IVE auf dem Clientcomputer des Benutzers die erforderliche Antivirenanwendung ausgeführt wird, wird der Benutzer Rolle A zugeordnet und erhält sämtliche zugehörigen Zugriffsmöglichkeiten. Wenn aber die Antivirenanwendung während der Benutzersitzung beendet wird, erfüllt der Benutzer bei der nächsten Ausführung von Host Checker die Sicherheitsanforderungen für Rolle A nicht mehr und verliert deshalb sämtliche Zugriffsberechtigungen für diese Rolle.

HINWEIS: Wenn Sie einen Wert von Null eingeben, wird Host Checker nur auf dem Clientcomputer ausgeführt, wenn sich der Benutzer erstmals an IVE anmeldet.

- Geben Sie im Feld **Client-side process, login inactivity timeout** ein Zeitbegrenzungsintervall an. Wenn der Benutzer die IVE-Anmeldeseite nach dem Starten von Host Checker und vor dem Anmelden am IVE verlässt, wird Host Checker auf dem Computer des Benutzers für die Dauer des von Ihnen festgelegten Intervalls ausgeführt.

- Aktivieren Sie die Option **Auto-upgrade Host Checker**, damit das IVE die Host Checker-Anwendung automatisch auf einen Clientcomputer herunterlädt, wenn die Host Checker-Version auf dem IVE neuer ist als die auf dem Client installierte Version. Beachten Sie bei Auswahl dieser Option Folgendes:

  - Unter Windows muss der Benutzer Administratorrechte besitzen, damit das IVE die Host Checker-Anwendung automatisch auf dem Client installiert. Weitere Informationen finden Sie unter „Erforderliche Berechtigungen zum Installieren und Ausführen von Anwendungen“ auf Seite 411.

  - Wenn ein Benutzer Host Checker deinstalliert und sich anschließend bei einem IVE anmeldet, für das die Option **Auto-upgrade Host Checker** nicht aktiviert ist, kann er nicht mehr auf Host Checker zugreifen.

- Aktivieren Sie **Perform dynamic policy reevaluation**, um die Rollen einzelner Benutzer automatisch zu aktualisieren, indem Sie die dynamische Richtlinienauswertung für Host Checker aktivieren. Host Checker kann das IVE veranlassen, bei jeder Änderung des Host Checker-Status eines Benutzers Ressourcenrichtlinien auszuwerten. (Wenn Sie diese Option nicht aktivieren, wertet das IVE Ressourcenrichtlinien nicht aus, es wertet aber die Authentifizierungsrichtlinien, Rollenzuordnungsregeln und Rolleneinschränkungen aus, sobald sich der Host Checker-Status eines Benutzers ändert.) Weitere Informationen finden Sie unter „Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)“ auf Seite 44.

- Aktivieren Sie **Create Host Checker Connection Control Policy**, um eine Verbindungssteuerungsrichtlinie zu erstellen, die Angriffe auf Windows-Clientcomputern von anderen infizierten Computern in demselben physischen Netzwerk verhindert. Die Verbindungssteuerungsrichtlinie blockiert alle eingehenden TCP-Verbindungen und alle ein- und ausgehenden UDP-Pakete. Diese Richtlinie lässt den gesamten ausgehenden TCP- und Network Connect-Verkehr sowie alle Verbindungen mit DNS-Servern, WINS-Servern, DHCP-Servern, Proxyservern und dem IVE zu.

HINWEIS: Wenn Sie die Option **Create Host Checker Connection Control Policy** aktivieren, müssen Sie auch die Verbindungssteuerungsrichtlinie auf der Bereichsebene auswerten bzw. erzwingen, damit die Richtlinie auf Clientcomputern wirksam wird. Unter Windows muss der Benutzer Administratorrechte besitzen, damit das IVE die Verbindungssteuerungsrichtlinie auf dem Clientcomputer erzwingt. Anweisungen hierfür finden Sie unter „Host Checker-Einschränkungen“ auf Seite 423.

3. Klicken Sie auf **Save Changes**.

Erstellen einer globalen clientseitigen Host Checker-Richtlinie

Für Clients mit Windows-, Macintosh- oder Linux-Betriebssystem können globale Host Checker-Richtlinien erstellt werden, die sicherstellen, dass bestimmte clientseitige Prozesse, Dateien und Ports Ihren Spezifikationen entsprechen. Für Clients mit dem Betriebssystem Windows können Sie auch Registrierungseinträge überprüfen und globale Host Checker-Richtlinien für integrierte Endpunktsicherheitsprodukte von Drittanbietern erstellen.

Nachdem Sie diese Richtlinien erstellt haben, können Sie sie auf Bereichs- und Rollenebene implementieren.

So erstellen Sie eine globale clientseitige Host Checker-Richtlinie:

1. Wählen Sie in der Webkonsole **Signing In > End Point > Host Checker**.
2. Klicken Sie unter **Policies** auf **New**.
3. Geben einen Namen im Feld **Policy Name** ein, und klicken Sie auf **Continue**. (Benutzer sehen diesen Namen auf der Host Checker-Hilfsoptionsseite, wenn Sie benutzerdefinierte Anweisungen für diese Richtlinie aktivieren.)
4. Klicken Sie auf die Registerkarte für das Betriebssystem, für das Sie Host Checker-Optionen festlegen möchten – **Windows**, **Mac** oder **Linux**. In einer Richtlinie können unterschiedliche Host Checker-Anforderungen für jedes Betriebssystem definiert werden. Sie können z. B. eine Richtlinie erstellen, die auf jedem Betriebssystem unterschiedliche Dateien oder Prozesse überprüft.
5. (Nur Windows) Wählen Sie unter **Host Checking Method** eine beliebige Anzahl der folgenden Optionen aus (optional):
   - **Sygate Enforcement API** – Zur Verwendung dieser Option muss das Produkt Sygate Personal Firewall auf dem Clientcomputer installiert sein.
   - **Sygate Security Agent** – Zur Verwendung dieser Option muss Sygate Security Agent auf dem Clientcomputer installiert sein.
   - **Zone Labs: Zone Alarm Pro and Zone Labs Integrity** – Zur Verwendung dieser Option muss entweder Zone Alarm Pro oder Zone Labs Integrity auf dem Clientcomputer installiert sein.
   - **McAfee Desktop Firewall 8.0** – Zur Verwendung dieser Option muss McAfee Desktop Firewall 8.0 auf dem Clientcomputer installiert sein.
   - **InfoExpress CyberGatekeeper Agent** – Zur Verwendung dieser Option muss das Produkt InfoExpress CyberGatekeeper Agent auf dem Clientcomputer installiert sein.

6. Wählen Sie unter **Rule Settings** in der Dropdownliste einen Regeltyp aus (Beschreibungen finden Sie unter „Richtlinien für Host Checker definieren“ auf Seite 76), und klicken Sie dann auf **Add** (optional). Das Konfigurationsdialogfeld für diese Regel wird angezeigt. Gehen Sie in den jeweiligen Konfigurationsdialogfeldern folgendermaßen vor:

   - **3rd Party NHC Check** (nur Windows):

     i. Geben Sie einen Namen für die Drittanbieter-NHC-Prüfungsregel ein.

     ii. Geben Sie den Speicherort der DLL auf den Clientcomputern (Pfad und Dateiname) an.

     iii. Klicken Sie auf **Save Changes**.

   - **Attribute Check: Ports**:

     i. Geben Sie einen Namen für die Portregel ein.

     ii. Geben Sie eine Liste von Ports mit Kommas als Trennzeichen (ohne Leerzeichen) oder einen Bereich von Ports ein, beispielsweise: 1234,11000-11999,1235.

     iii. Wählen Sie **Required**, um zu bestimmen, dass diese Ports auf dem Clientcomputer geöffnet sein müssen, oder **Deny**, um zu bestimmen, dass sie geschlossen sein müssen.

     iv. Klicken Sie auf **Save Changes**.

   - **Attribute Check: Process**:

     i. Geben Sie einen Namen für die Prozessregel ein.

     ii. Geben Sie den Namen eines Prozesses (ausführbare Datei) ein, beispielsweise: good-app.exe.

     Für den Prozessnamen können Platzhalterzeichen verwendet werden. Beispiel:

     good*.exe

Weitere Informationen finden Sie unter „Verwenden von Platzhaltern oder Umgebungsvariablen in einer Host Checker-Regel“ auf Seite 214.

iii. Wählen Sie **Required** aus, um festzulegen, dass dieser Prozess ausgeführt werden muss, oder wählen Sie **Deny** aus, damit dieser Prozess nicht ausgeführt wird.

iv. Geben Sie den MD5-Prüfsummenwert für jede der ausführbaren Dateien ein, auf die die Richtlinie angewendet werden soll (optional). Beispielsweise kann eine ausführbare Datei auf einem Desktop, einem Laptop oder verschiedenen Betriebssystemen unterschiedliche MD5-Prüfsummenwerte aufweisen. Unter Macintosh und Linux können Sie die MD5-Prüfsumme mit folgendem Befehl ermitteln:

```
openssl md5 <Prozessdateipfad>
```

v. Klicken Sie auf **Save Changes**.

- **Attribute Check: File**:

i. Geben Sie einen Namen für die Dateiregel ein.

ii. Geben Sie den Namen einer Datei (eines beliebigen Dateityps) ein, beispielsweise: `c:\temp\bad-file.txt` oder `/temp/bad-file.txt`.

Für den Dateinamen können Platzhalterzeichen verwendet werden. Beispiel:

```
*.txt
```

Sie können den Verzeichnispfad der Datei auch mit einer Umgebungsvariable angeben. (Im Verzeichnispfad dürfen keine Platzhalterzeichen verwendet werden.) Schließen Sie die Variable in die Zeichen <% und %> ein. Beispiel:

```
<%windir%>\bad-file.txt
```

Weitere Informationen finden Sie unter „Verwenden von Platzhaltern oder Umgebungsvariablen in einer Host Checker-Regel“ auf Seite 214.

iii. Wählen Sie **Required** aus, um zu fordern, dass diese Datei auf dem Clientcomputer vorhanden ist, oder wählen Sie **Deny** aus, um zu fordern, dass diese Datei nicht vorhanden ist.

iv. Geben Sie das maximale Alter der Datei in Tagen an (optional). Wenn die Datei älter als die angegebene Anzahl von Tagen ist, entspricht der Client nicht den Anforderungen der Attributprüfung.

HINWEIS: Mit der Option für das maximale Alter kann das Alter von Virensignaturen überprüft werden. Geben Sie (im Feld **File Name**) den Pfad einer Datei an, deren Zeitstempel die letzte Aktualisierung der Virensignaturen angibt, z. B eine Virensignaturdatenbank oder eine Protokolldatei, die bei jeder Aktualisierung der Datenbank ebenfalls aktualisiert wird. Wenn Sie beispielsweise TrendMicro verwenden, können Sie Folgendes angeben:

C:\Programme\Trend Micro\OfficeScan Client\TmUpdate.ini.

v. Geben Sie den MD5-Prüfsummenwert für jede Datei ein, auf die die Richtlinie angewendet werden soll (optional). Unter Macintosh und Linux können Sie die MD5-Prüfsumme mit folgendem Befehl ermitteln:

```
openssl md5 <Dateipfad>
```

vi. Klicken Sie auf **Save Changes**.

- **Attribute Check: Registry Setting** (nur Windows):

i. Geben Sie einen Namen für die Registrierungseinstellungsregel ein.

ii. Wählen Sie in der Dropdownliste einen Stammschlüssel aus.

iii. Geben Sie den Pfad zum Anwendungsordner für den Registrierungsteilschlüssel ein.

iv. Geben Sie den Namen des Schlüsselwertes ein, der gefordert werden soll (optional). Dieser Name wird in der Spalte **Name** des Registrierungs-Editors angezeigt.

v. Wählen Sie in der Dropdownliste den Typ des Schlüsselwertes aus (**String**, **Binary** oder **DWORD**) (optional). Dieser Typ wird in der Spalte **Type** des Registrierungseditors angezeigt.

vi. Geben Sie den geforderten Registrierungsschlüsselwert an (optional). Diese Informationen werden in der Spalte **Data** des Registrierungseditors angezeigt.

Wenn der Schlüsselwert für eine Anwendungsversion steht, aktivieren Sie **Minimum version**, um die angegebene Version oder neuere Versionen der Anwendung zuzulassen. Das IVE verwendet lexikalisches Sortieren, um zu bestimmen, ob der Client die angegebene oder eine neuere Version enthält. Beispiel:

3.3.3 ist neuer als 3.3

4.0 ist neuer als 3.3

4.0a ist neuer als 4.0b

4.1 ist neuer als 3.3.1

HINWEIS: Mit dieser Option können Sie Versionsinformationen für eine Antivirenanwendung angeben, um sicherzustellen, dass die Antivirensoftware des Clients aktuell ist.

vii. Klicken Sie auf **Save Changes**.

HINWEIS: Wenn Sie lediglich den Schlüssel und den Teilschlüssel angeben, überprüft Host Checker einfach, ob der Ordner „Subkey“ in der Registrierung vorhanden ist.

7. Wiederholen Sie ggf. Schritt 6, um der Richtlinie weitere Regeln hinzuzufügen.

8. Wenn Sie in der Richtlinie alternative Regelsätze verwenden möchten, aktivieren Sie neben **Rules expression** die Option **Edit**, um Regeln mit booleschen Operatoren (AND, OR) zu kombinieren. Beachten Sie bei der Eingabe von Regelausdrücken folgende Richtlinien:

   - Geben Sie den Namen der Regeln ins Textfeld **Rules expression** ein.
   - Verwenden Sie AND, wenn zwei Regeln oder Regelsätze zutreffen müssen.
   - Verwenden Sie OR, wenn eine von zwei Regeln oder einer von zwei Regelsätzen zutreffen muss.
   - Verwenden Sie Klammern zum Kombinieren von Regelsätzen.

   Mit dem folgenden Ausdruck können Sie z. B. die Ausführung einer persönlichen Firewall und die Ausführung von einem von zwei möglichen Antivirenprodukten erzwingen:

   ZoneLabsFirewall AND (McAfeeAntivirus OR NortonAntivirus)

9. Legen Sie die Korrekturaktionen fest (siehe „Host Checker-Hilfsoption verwenden“ auf Seite 78), die Host Checker ausführen soll, wenn der Computer eines Benutzers nicht den Anforderungen der aktuellen Richtlinie entspricht (optional):

- **Enable Custom Instructions** – Geben Sie die Anweisungen ein, die auf der Host Checker-Hilfsoptionsseite für den Benutzer angezeigt werden sollen. Sie können den Text mit den folgenden HTML-Tags formatieren und Links zu Ressourcen hinzufügen, z. B. Richtlinienservern oder Websites: <i>, <b>, <br>, <font> und <a href>. Beispiel:

  Sie verfügen nicht über die aktuellsten Signaturdateien.
  Klicken Sie hier, um die neuesten Signaturdateien herunterzuladen.

HINWEIS: Wenn Sie für Windows-Clients einen Link zu einem IVE-geschützten Richtlinienserver in die Anweisungen einfügen, müssen Sie einen Tunnel für den Zugriff vor der Authentifizierung definieren. Informationen hierzu finden Sie unter „Festlegen von Host Checker-Tunneldefinitionen für den Zugriff vor der Authentifizierung“ auf Seite 216.

- **Evaluate other policies** – Sie können alternative Richtlinien auswählen, die Host Checker auswertet, wenn der Computer des Benutzers die aktuellen Richtlinienanforderungen nicht erfüllt. Wenn ein Benutzer z. B. versucht, über einen externen Clientcomputer (z. B. einen Kiosk) auf das IVE zuzugreifen, können Sie mit dieser Option festlegen, dass eine andere Richtlinie ausgewertet wird, gemäß derer der Benutzer in einer Sygate Virtual Desktop-Umgebung auf das IVE zugreifen muss. Wählen Sie in der Liste **HC Policies** die alternative Richtlinie aus, und klicken Sie dann auf **Add**.

HINWEIS: Wenn Sie für eine alternative Richtlinie ebenfalls eine eigene alternative Richtlinie konfigurieren, wertet Host Checker diese alternative Richtlinie auf „sekundärer Ebene“ nicht für die aktuelle Richtlinie aus. Host Checker wertet also nur eine alternative Richtlinie pro Transaktion aus.

- **Kill Process** – Geben Sie in jeder Zeile den Namen der Prozesse ein, die beendet werden sollen, wenn der Computer des Benutzers nicht den Richtlinienanforderungen entspricht. Sie können eine optionale MD5-Prüfsumme für den Prozess hinzufügen. (Platzhalter sind nicht zulässig für die Prozessnamen.) Beachten Sie, dass der Benutzer über entsprechende Berechtigungen zum Beenden des Prozesses verfügen muss. Beispiel:

  keylogger.exe
  MD5: 6A7DFAF12C3183B56C44E89B12DBEF56

- **Delete Files** – Geben Sie die Namen der Dateien ein, die gelöscht werden sollen, wenn der Computer des Benutzers nicht den Richtlinienanforderungen entspricht. (Platzhalter sind nicht zulässig für die Dateinamen.) Geben Sie einen Dateinamen pro Zeile ein. Beachten Sie, dass der Benutzer über entsprechende Berechtigungen zum Löschen der Datei verfügen muss. Beispiel:

  c:\temp\bad-file.txt
  /temp/bad-file.txt

10. Wenn Sie in dieser Richtlinie für ein anderes Betriebssystem Regeln hinzufügen oder Host Checker-Optionen festlegen möchten, wiederholen Sie Schritt 4 bis Schritt 9.

11. Klicken Sie anschließend auf der Seite **Signing In > End Point > Host Checker** auf **Save Changes**. Das IVE fügt die Richtlinie der Seite **Host Checker Configuration** hinzu.

12. Verwenden Sie zum Implementieren der Richtlinien auf Bereichs-, Rollen- und Ressourcenrichtlinienebene die unter „Host Checker-Einschränkungen“ auf Seite 423 beschriebenen Optionen.

Verwenden von Platzhaltern oder Umgebungsvariablen in einer Host Checker-Regel

Die folgenden Platzhalter können verwendet werden, um einen Dateinamen in einer **Attribute Check: File**-Regel oder einen Prozessnamen in einer **Attribute Check: Process**-Regel anzugeben:

Tabelle 6: Platzhalterzeichen für die Angabe von Datei- oder Prozessnamen

Platzhalterzeichen	Beschreibung	Beispiel
*	Entspricht einem beliebigen Zeichen	*.txt
?	Entspricht genau einem Zeichen	app-?.exe

In einer **Attribute Check: File**-Regel für Windows können die folgenden Umgebungsvariablen zum Angeben des Verzeichnispfads einer Datei verwendet werden:

Tabelle 7: Umgebungsvariablen für die Angabe eines Verzeichnispfads unter Windows

Umgebungsvariable	Windows-Beispielwert
<%APPDATA%>	C:\Dokumente und Einstellungen\jdoe\Anwendungsdaten
<%windir%>	C:\WINDOWS
<%ProgramFiles%>	C:\Programme
<%CommonProgramFiles%>	C:\Programme\Gemeinsame Dateien
<%USERPROFILE%>	C:\Dokumente und Einstellungen\jdoe
<%HOMEDRIVE%>	C:
<%Temp%>	C:\Dokumente und Einstellungen\ < Benutzername > \Lokale Einstellungen\Temp

In einer **Attribute Check: File**-Regel für Macintosh oder Linux können die folgenden Umgebungsvariablen zum Angeben des Verzeichnispfads einer Datei verwendet werden:

Tabelle 8: Umgebungsvariablen für die Angabe eines Verzeichnispfads unter Macintosh und Linux

Umgebungsvariable	Macintosh-Beispielwert	Linux-Beispielwert
<%java.home%>	/System/Library/Frameworks/JavaVM. framework/ Versions/1.4.2/Home	/local/local/java/j2sdk1.4.1_02/jre
<%java.io.tmpdir%>	/tmp	/tmp
<%user.dir%>	/Users/admin	/home-shared/cknouse
<%user.home%>	/Users/admin	/home/cknouse

Erstellen einer globalen Serverrichtlinie

Für Windows-Clients können globale Host Checker-Richtlinien erstellt werden, die eine auf das IVE hochgeladene J.E.D.I.-DLL abrufen und auf Clientcomputern ausführen. Nachdem Sie diese Richtlinien erstellt haben, können Sie sie auf Bereichs-, Rollen- und Ressourcenebene aufrufen. Weitere Informationen finden Sie unter „Richtlinien für Host Checker definieren“ auf Seite 76.

So erstellen Sie eine globale serverseitige Host Checker-Richtlinie:

1. Wählen Sie in der Webkonsole **Signing In > End Point > Host Checker**.
2. Klicken Sie unter **Policies** auf **New 3rd Party Policy**.
3. Geben Sie einen Namen ein, um Ihre ZIP-Datei im IVE zu bezeichnen.
4. Navigieren Sie zu dem lokalen Verzeichnis, in dem sich Ihre ZIP-Datei befindet.
5. Legen Sie die Korrekturaktionen fest (siehe „Host Checker-Hilfsoption verwenden“ auf Seite 78), die Host Checker ausführen soll, wenn der Computer eines Benutzers nicht den Anforderungen der aktuellen Richtlinie entspricht (optional):

   - **Enable Custom Instructions** – Geben Sie die Anweisungen ein, die auf der Host Checker-Hilfsoptionsseite für den Benutzer angezeigt werden sollen. Sie können den Text mit den folgenden HTML-Tags formatieren und Links zu Ressourcen hinzufügen, z. B. Richtlinienservern oder Websites: <i>, <b>, <br>, <font> und <a href>. Beispiel:

     Sie verfügen nicht über die aktuellsten Signaturdateien.
     Klicken Sie hier, um die neuesten Signaturdateien herunterzuladen.

HINWEIS: Wenn Sie für Windows-Clients einen Link zu einem IVE-geschützten Richtlinienserver in die Anweisungen einfügen, müssen Sie einen Tunnel für den Zugriff vor der Authentifizierung definieren. Informationen hierzu finden Sie unter „Festlegen von Host Checker-Tunneldefinitionen für den Zugriff vor der Authentifizierung“ auf Seite 216.

- **Evaluate other policies** – Sie können alternative Richtlinien auswählen, die Host Checker auswertet, wenn der Computer des Benutzers die aktuellen Richtlinienanforderungen nicht erfüllt. Wenn ein Benutzer z. B. versucht, über einen externen Clientcomputer (z. B. einen Kiosk) auf das IVE zuzugreifen, können Sie mit dieser Option festlegen, dass eine andere Richtlinie ausgewertet wird, gemäß derer der Benutzer in einer Sygate Virtual Desktop-Umgebung auf das IVE zugreifen muss. Wählen Sie in der Liste **HC Policies** die alternative Richtlinie aus, und klicken Sie dann auf **Add**.

HINWEIS: Wenn Sie für eine alternative Richtlinie ebenfalls eine eigene alternative Richtlinie konfigurieren, wertet Host Checker diese alternative Richtlinie auf „sekundärer Ebene“ nicht für die aktuelle Richtlinie aus. Host Checker wertet also nur eine alternative Richtlinie pro Transaktion aus.

- **Remediate** – Mit dieser Option können Sie über die Remediate () API-Funktion in einer J.E.D.I.-DLL eines Drittanbieters festgelegte Korrekturaktionen ausführen. Weitere Informationen finden Sie in dem auf der Juniper Support-Site verfügbaren *J.E.D.I. Solution Guide*.

- **Kill Process** – Geben Sie in jeder Zeile den Namen der Prozesse ein, die beendet werden sollen, wenn der Computer des Benutzers nicht den Richtlinienanforderungen entspricht. Sie können eine optionale MD5-Prüfsumme für den Prozess hinzufügen. (Platzhalter sind nicht zulässig für die Prozessnamen.) Beispiel:

  keylogger.exe
  MD5: 6A7DFAF12C3183B56C44E89B12DBEF56

- **Delete Files** – Geben Sie die Namen der Dateien ein, die gelöscht werden sollen, wenn der Computer des Benutzers nicht den Richtlinienanforderungen entspricht. (Platzhalter sind nicht zulässig für die Dateinamen.) Geben Sie einen Dateinamen pro Zeile ein. Beispiel:

  c:\temp\bad-file.txt
  /temp/bad-file.txt

6. Klicken Sie auf **Save Changes**. Das IVE fügt die in Ihrer ZIP-Datei definierten Richtlinien der Seite Host Checker **Configuration** hinzu.

7. Verwenden Sie zum Implementieren der Richtlinien auf Bereichs-, Rollen- und Ressourcenrichtlinienebene die unter „Host Checker-Einschränkungen“ auf Seite 423 beschriebenen Optionen.

Festlegen von Host Checker-Tunneldefinitionen für den Zugriff vor der Authentifizierung

Für Windows-Clients können Sie einen Tunnel für den Zugriff vor der Authentifizierung festlegen, der Host Checker-Methoden oder J.E.D.I.-DLLs von Drittanbietern vor der Authentifizierung von Benutzern den Zugriff auf einen IVE-geschützten Richtlinienserver (oder eine andere Ressource) ermöglicht. (Weitere Informationen finden Sie unter „Richtlinienserver für Host Checker-Clients verfügbar machen“ auf Seite 82.)

Eine Definition für einen Host Checker-Tunnel für den Zugriff vor der Authentifizierung konfiguriert den Zugriff auf einen Richtlinienserver oder eine andere Ressource. Jede Tunneldefinition besteht aus einem Paar von IP-Adressen und Ports: einer Loopback-IP-Adresse und einem Port auf dem Client und einer IP-Adresse und einem Port auf dem Richtlinienserver.

Tunneldefinitionen werden in einer Paketdefinitionsdatei für Host Checker-Richtlinien festgelegt. Diese Paketdefinitionsdatei, die den Namen MANIFEST.HCIF erhalten muss, definiert den Namen einer Schnittstellen-DLL, die in der DLL definierten Host Checker-Richtlinien und die Tunneldefinitionen für den Zugriff vor der Authentifizierung. Wenn das Paket keine Richtlinien enthält, erzwingt Host Checker lediglich die Ausführung des Pakets auf dem Client. Wenn Sie Richtlinien über diese Datei deklarieren, sind die Richtlinien in der IVE-Webkonsole verfügbar und können auf der Bereichs-, Rollen- oder Ressourcenebene implementiert werden.

In der Datei MANIFEST.HCIF muss eine Definition auf jeweils einer Zeile eingegeben werden, und die einzelnen Definitionen müssen durch eine leere Zeile getrennt werden. Verwenden Sie das folgende Format:

HCIF-Main : <DLLName>
HCIF-Policy : <Richtlinienname>
HCIF-IVE-Tunnel: <Client-Loopback>:port <Richtlinienserver>:port

Dabei ist:

<DLLName> der Name der Schnittstellen-DLL, z. B. myPestPatrol.dll. Auch wenn Sie keine Schnittstellen-DLL verwenden, müssen Sie eine Dummy-DLL als Platzhalterdatei mit genau diesem Namen angeben.

<Richtlinienname> der Name der in der DLL definierten Richtlinie, z. B. myFileCheck. Sie können mehrere Richtlinien definieren, indem Sie für jede Richtlinie die HCIF-Policy-Anweisung verwenden. Wenn Sie keine Schnittstellen-DLL verwenden, können Sie einen beliebigen Richtliniennamen als Platzhalter angeben.

Die Syntax einer Host Checker-Tunneldefinition lautet wie folgt:

HCIF-IVE-Tunnel: <Client-Loopback>:port <Richtlinienserver>:port

Dabei ist:

<Client-Loopback> eine Loopbackadresse, die mit 127. beginnt und in einen der folgenden Formen angegeben wird:

- Ein Hostname, der in eine mit 127 beginnende Loopbackadresse aufgelöst wird. Sie können zum Auflösen der Loopbackadresse eine lokale Hostdatei auf jedem Clientcomputer oder einem DNS-Server verwenden.

- Ein Hostname, der nicht zu einer Loopbackadresse aufgelöst wird oder zu einer Nicht-Loopbackadresse aufgelöst wird. In diesen Fällen ordnet Host Checker eine Loopbackadresse zu, und die lokale Hostdatei auf dem Client wird mit der Zuordnung aktualisiert. Der Benutzer muss Administratorrechte besitzen, damit Host Checker die lokale Hostdatei ändern kann. Wenn der Benutzer nicht über Administratorrechte verfügt, kann Host Checker die Hostdatei nicht aktualisieren und den Tunnel für den Zugriff vor der Authentifizierung nicht öffnen. In diesem Fall zeichnet Host Checker einen Fehler im Protokoll auf.

<Richtlinienserver> die IP-Adresse oder der Hostname des Back-End-Richtlinienservers. Das IVE löst den von Ihnen angegebenen Hostnamen auf.

In der folgenden Tunneldefinition gibt 127.0.0.1:3220 z. B. die Loopbackadresse und den Port des Clients an, und mysygate.company.com:5500 steht für den Hostnamen und Port des Richtlinienservers:

```
HCIF-IVE-Tunnel:  127.0.0.1:3220    mysygate.company.com:5500
```

Sie können auch wie im folgenden Beispiel einen Hostnamen für den Client verwenden:

```
HCIF-IVE-Tunnel:  mysygate.company.com:3220    mysygate.company.com:5500
```

Beachten Sie beim Festlegen von Tunneldefinitionen Folgendes:

- Sie müssen eine leere Zeile zwischen den einzelnen Definitionszeilen in der Datei MANIFEST.HCIF hinzufügen, und Sie können Kommentare durch ein Semikolon am Zeilenanfang kennzeichnen. Beispiel:

  ```
  HCIF-Main : myPestPatrol.dll
  HCIF-Policy : myFileCheck
  HCIF-Policy : myPortCheck
  ; Tunneldefinitionen
  HCIF-IVE-Tunnel:  127.0.0.1:3220    mysygate.company.com:5500
  HCIF-IVE-Tunnel:  127.1.1.1:3220    mysygate2.company.com:5500
  HCIF-IVE-Tunnel:  mysygate.company.com:3220    mysygate3.company.com:5500
  ```

- Host Checker-Tunnel für den Zugriff vor der Authentifizierung werden nur unter Windows unterstützt.

- Wenn <Client-Loopback> eine Nicht-Loopbackadresse ist, kann Host Checker den Tunnel für den Zugriff vor der Authentifizierung nicht öffnen, und stattdessen wird ein Fehler ausgegeben.

- Wenn Sie eine andere Loopbackadresse als 127.0.0.1 verwenden (z. B. 127.0.0.2 und höher), müssen Clients mit Windows XP Service Pack 2 den Hotfix für XP SP2 installieren. Siehe:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;884020

HINWEIS: Beim Bereitstellen einer client- oder serverseitigen Drittanbieter-DLL ist Folgendes zu beachten:

- Dekomprimieren Sie das Paket mit der serverseitigen Drittanbieter-DLL, und fügen Sie der Datei MANIFEST.HCIF Tunneldefinitionen mit den Richtlinien für die Drittanbieter-DLL hinzu. (Die DLL muss die in der Datei MANIFEST.HCIF angegebene <Client-Loopback>-Adresse und den gleichen Port oder Hostname verwenden.)

- Da ein Tunnel für den Zugriff vor der Authentifizierung nur während der Ausführung von Host Checker geöffnet ist, kann eine Drittanbieter-DLL nur dann auf den IVE-geschützten Richtlinienserver zugreifen, wenn Host Checker ausgeführt wird.

- Stellt eine Drittanbieter-DLL die Verbindung mit ihrem Richtlinienserver mittels HTTPS und über einen korrekt zur Loopbackadresse aufgelösten Hostnamen her, werden keine Serverzertifikatswarnungen angezeigt. Wenn die Drittanbieter-DLL die Verbindung jedoch explizit über eine Loopbackadresse herstellt, werden Serverzertifikatswarnungen angezeigt, da der Hostname im Zertifikat nicht mit der Loopbackadresse übereinstimmt. (Der Entwickler der Drittanbieter-DLL kann die DLL so konfigurieren, dass sie diese Warnungen ignoriert.)

Weitere Informationen zu Drittanbieter-DLLs finden Sie in dem auf der Juniper Support-Site verfügbaren *J.E.D.I. Solution Guide*.

Hochladen eines Host Checker-Richtlinienpakets in das IVE

Damit das IVE eine Paketdefinitionsdatei erkennen kann, muss der Datei der Name MANIFEST.HCIF zugewiesen werden, und sie muss in einem Ordner namens META-INF gespeichert werden. Anschließend müssen Sie den Ordner META-INF mit der Datei MANIFEST.HCIF zusammen mit der Schnittstellen-DLL und allen Intialisierungsdateien in einer ZIP-Datei für das Host Checker-Richtlinienpaket archivieren. Die ZIP-Datei für ein Host Checker-Richtlinienpaket kann z. B. Folgendes enthalten:

META-INF/MANIFEST.HCIF
hcif-myPestPatrol.dll
hcif-myPestPatrol.ini

Sie können mehrere Richtlinienpakete mit einer jeweils unterschiedlichen Datei MANIFEST.HCIF in das IVE laden. Host Checker erstellt unter der Annahme, dass alle Definitionen eindeutig sind, Tunnel für alle Tunneldefinitionen in allen MANIFEST.HCIF-Dateien.

So laden Sie das Host Checker-Richtlinienpaket in das IVE hoch:

1. Wählen Sie in der Webkonsole **Signing In > End Point > Host Checker**.
2. Klicken Sie unter **Policies** auf **New 3rd Party Policy**.
3. Geben Sie einen Namen zur Identifizierung des Host Checker-Richtlinienpakets auf dem IVE ein. Beispielsweise myPestPatrol.

4. Wechseln Sie zu dem lokalen Verzeichnis, auf dem die ZIP-Datei für das Host Checker-Richtlinienpaket gespeichert ist.

5. Klicken Sie auf **Save Changes**. Das IVE fügt das Host Checker-Richtlinienpaket auf der Seite **Host Checker Configuration** unter **3rd Party Policy** hinzu. Wenn Sie die Liste der Tunneldefinitionen für den Zugriff vor der Authentifizierung für ein Richtlinienpaket anzeigen möchten, klicken Sie auf der Seite **Host Checker Configuration** unter **3rd Party Policy** auf den Namen des gewünschten Pakets. Das IVE listet die Tunneldefinitionen auf der Seite **3rd Party Policy** unter **Host Checker Preauth Access Tunnels** auf.

Nachdem ein Host Checker-Richtlinienpaket in das IVE hochgeladen wurde, kann es auf dem Server nicht mehr geändert werden. Das Paket muss auf dem lokalen System bearbeitet werden, und die geänderte Version muss dann in das IVE hochgeladen werden.

HINWEIS: Nachdem Sie ein Host Checker-Richtlinienpaket in das IVE hochgeladen haben, können Sie das Paket bzw. die Richtlinien in einer Bereichs-, Rollen- oder Ressourcenrichtlinie auswerten oder erzwingen. Wenn das Paket selbst auf dem Clientcomputer installiert und ausgeführt werden soll (im Gegensatz zu einer bestimmten erfüllten oder nicht eingehaltenen Richtlinie im Paket), können Sie den beim Hochladen des Richtlinienpakets angegebenen Namen verwenden (z. B. myPestPatrol). Verwenden Sie zum Erzwingen einer bestimmten Richtlinie im Paket die Syntax <Paketname>.<Richtlinienname>. Wenn Sie z. B. die Richtlinie FileCheck im Paket myPestPatrol erzwingen möchten, geben Sie myPestPatrol.FileCheck an. Anweisungen hierfür finden Sie unter „Host Checker-Einschränkungen“ auf Seite 423.

Herunterladen des Host Checker-Installationsprogramms

Wählen Sie **Maintenance > System > Installers** aus, um die Host Checker-Anwendung als ausführbare Windows-Datei herunterzuladen. Weitere Informationen über das Herunterladen von Host Checker finden Sie unter „Herunterladen von Anwendungen oder Diensten“ auf Seite 362.

Registerkarte „Cache Cleaner“

Auf der Registerkarte **Signing In > End Point > Cache Cleaner** können Sie festlegen, wie oft Cache Cleaner ausgeführt wird und das IVE über den Status informiert. Darüber hinaus können Sie zu löschende Cachedaten des Browsers und Verzeichnisdaten angeben. Weitere Informationen über diese Funktion finden Sie unter „Cache Cleaner – Übersicht“ auf Seite 87.

Festlegen globaler Einstellungen für Cache Cleaner

So geben Sie globale Einstellungen für Cache Cleaner an:

1. Wählen Sie in der Webkonsole **Signing In > End Point > Cache Cleaner**.

2. Geben Sie unter **Options** Folgendes an:

   a. Geben Sie im Feld **Cleaner Frequency** an, wie oft Cache Cleaner ausgeführt wird. Gültige Werte liegen zwischen 1 und 60 Minuten. Bei jeder Ausführung von Cache Cleaner werden der gesamte über das IVE-Modul für die Inhaltsvermittlung heruntergeladene Inhalt sowie der Cache des Browsers und die unten in den Bereichen **Browser Cache** und **Files and Folders** angegebenen Dateien und Ordner gelöscht.

   b. Geben Sie im Feld **Status Update Frequency** an, wie oft das IVE erwartet, dass die Cachebereinigung sich selbst aktualisiert. Gültige Werte liegen zwischen 1 und 60 Minuten.

   c. Geben Sie im Feld **Client-side process, login inactivity timeout** ein Zeitbegrenzungsintervall an. Wenn der Benutzer die IVE-Anmeldeseite nach dem Starten von Cache Cleaner und vor dem Anmelden am IVE verlässt, wird Cache Cleaner auf dem Computer des Benutzers für die Dauer des von Ihnen festgelegten Intervalls ausgeführt.

   d. Aktivieren Sie das Kontrollkästchen **Disable AutoComplete of web addresses**, um den Browser daran zu hindern, Webadressen während einer IVE-Sitzung des Benutzers automatisch mit zwischengespeicherten Werten auszufüllen.

      Bei Verwendung dieser Option stellt das IVE den folgenden Windows-Registrierungswert während der IVE-Sitzung des Benutzers auf „0“ ein: HKEY_CURRENT_USER\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\ AutoComplete. Am Ende der Sitzung wird der Registrierungswert wieder auf die ursprüngliche Einstellung zurückgesetzt.

   e. Aktivieren Sie das Kontrollkästchen **Disable AutoComplete of usernames and passwords**, um zu verhindern, dass Internet Explorer Anmeldedaten von Benutzern mittels zwischengespeicherter Werte automatisch in Webformulare eingibt. Bei Auswahl dieser Option wird auch die Aufforderung „Kennwort speichern?” auf Windows-Systemen deaktiviert. Wenn Sie diese Option aktivieren, stellt das IVE die folgenden Windows-Registrierungswerte auf „0“:

      - HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FormSuggest Passwords
      - HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FormSuggest Passwords\FormSuggest PW Ask
      - HKEY_CURRENT_USER\SOFTWARE\Microsoft\ Windows\CurrentVersion\Internet Settings\ DisablePasswordCaching

f. Aktivieren Sie das Kontrollkästchen **Flush all existing AutoComplete Passwords**, um alle von Internet Explorer auf dem System des Benutzers zwischengespeicherten Kennwörter zu löschen. Wenn Sie diese Option aktivieren, stellt das IVE den folgenden Windows-Registrierungswert auf „0“: HKEY_CURRENT_USER \Software\\Microsoft\\Internet Explorer\\IntelliForms\\SPW

   Wählen Sie dann eine der folgenden Optionen:

   - Aktivieren Sie **For IVE session only**, damit das IVE die zwischengespeicherten Kennwörter des Benutzers am Ende dieser IVE-Sitzung wiederherstellt.
   - Wählen Sie **Permanently**, um die zwischengespeicherten Kennwörter des Benutzers dauerhaft zu löschen.

g. Aktivieren Sie das Kontrollkästchen **Uninstall Cache Cleaner at logout**, wenn das IVE Cache Cleaner beim Beenden einer Benutzersitzung vom Clientcomputer entfernen soll.

3. Geben Sie unter **Browser Cache** einen oder mehrere Hostnamen oder Domänen ein (Platzhalter sind zulässig). Beim Beenden einer Benutzersitzung entfernt Cache Cleaner den gesamten Inhalt des Browsercaches, der von diesen Servern stammt. Cache Cleaner entfernt diesen Inhalt auch, wenn sie im angegebenen Bereinigungsintervall ausgeführt wird. Das IVE löst Hostnamen nicht auf. Geben Sie deshalb alle möglichen Angaben für einen Server ein, z. B. seinen Hostnamen, FQDN und die IP-Adresse.

4. Führen Sie unter **Files and Folders** Folgendes aus:

   a. Geben Sie eine der folgenden Informationen an:

      - den Namen der Datei, die von Cache Cleaner entfernt werden soll, oder
      - den vollständigen Verzeichnispfad zu einem Ordner, dessen Inhalt von Cache Cleaner entfernt werden soll. Wenn Sie ein Verzeichnis angeben, wählen Sie **Clear Subfolders** aus, um auch den Inhalt aller Unterverzeichnisse in diesem Verzeichnis zu löschen.

   b. Aktivieren Sie das Kontrollkästchen **Clear folders only at the end of session**, wenn Cache Cleaner den Verzeichnisinhalt nur nach dem Beenden der Benutzersitzung löschen soll. Andernfalls löscht Cache Cleaner auch Dateien und Ordner im angegebenen Bereinigungsintervall.

5. Klicken Sie zum globalen Speichern der Einstellungen auf **Save Changes**.

HINWEIS: Für Internet Explorer löscht Cache Cleaner unabhängig von den unter **Files and Folders** angegebenen Verzeichnissen automatisch den *gesamten* Cacheinhalt. Für Firefox löscht Cache Cleaner *nur* die unter **Files and Folders** angegebenen Verzeichnisse.

Konfigurieren der Seite „AAA Servers“

Auf der Seite **AAA Servers** können Sie Authentifizierungsserver konfigurieren. Weitere Informationen hierzu finden Sie unter:

- „Definieren einer Authentifizierungsserverinstanz“ auf Seite 224
- „Ändern einer Authentifizierungsserverinstanz“ auf Seite 224
- „Konfigurieren einer lokalen Authentifizierungsserverinstanz“ auf Seite 225
- „Konfigurieren einer LDAP-Serverinstanz“ auf Seite 230
- „Konfigurieren einer NIS-Serverinstanz“ auf Seite 233
- „Konfigurieren einer ACE/Serverinstanz“ auf Seite 234
- „Konfigurieren einer RADIUS-Serverinstanz“ auf Seite 238
- „Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz“ auf Seite 245
- „Konfigurieren einer Instanz eines anonymen Servers“ auf Seite 250
- „Konfigurieren einer Zertifikatserverinstanz“ auf Seite 252
- „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 254

HINWEIS: Beachten Sie bei der Auswahl des Servertyps Folgendes:

- Sie können nur eine ACE- und eine RADIUS-Serverinstanz pro IVE erstellen.
- Sie können den Active Directory-Server mit folgenden Protokollen authentifizieren:
  - **NTLM-Protokoll** – Wählen Sie **Active Directory/Windows NT Domain** aus. Weitere Informationen finden Sie unter „Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz“ auf Seite 245.
  - **LDAP-Protokoll** – Wählen Sie **LDAP Server** aus. Weitere Informationen finden Sie unter „Konfigurieren einer LDAP-Serverinstanz“ auf Seite 230.
- Wenn Sie eine lokale IVE-Serverinstanz zum Authentifizieren von Benutzeradministratoren erstellen, müssen Sie **IVE Authentication** auswählen. Weitere Informationen finden Sie unter „Konfigurieren einer lokalen Authentifizierungsserverinstanz“ auf Seite 225.

Definieren einer Authentifizierungsserverinstanz

Diese Seite dient zum Definieren von Authentifizierungsserverinstanzen. Authentifizierungsserver authentifizieren Anmeldeinformationen der Benutzer, während Autorisierungsserver Benutzerinformationen bereitstellen, die das IVE zur Ermittlung von Benutzerberechtigungen im System verwendet. Sie können z. B. eine Zertifikatserverinstanz angeben, die Benutzer anhand ihrer clientseitigen Zertifikatsattribute authentifiziert, und dann eine LDAP-Serverinstanz erstellen, die Benutzer anhand der Werte autorisiert, die in einer Zertifikatsperrliste (Certificate Revocation List, CRL) aufgeführt sind. Weitere Informationen zu Authentifizierungsservern finden Sie unter „Authentifizierungsserver“ auf Seite 51.

So definieren Sie eine Authentifizierungsserverinstanz:

1. Wählen Sie im Dropdownmenü **New** einen Servertyp aus.
2. Klicken Sie auf **Go**.
3. Legen Sie entsprechend dem ausgewählten Server Einstellungen für die Serverinstanz fest.
4. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll. Weitere Informationen finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich“ auf Seite 260.
5. Wenn Sie den lokalen IVE-Authentifizierungsserver konfigurieren, müssen Sie lokale Benutzerkonten festlegen. Anweisungen hierfür finden Sie unter „Konfigurieren einer lokalen Authentifizierungsserverinstanz“ auf Seite 225.

Ändern einer Authentifizierungsserverinstanz

So ändern Sie eine Authentifizierungsserverinstanz:

1. Wählen Sie **Signing In > AAA Servers**.
2. Klicken Sie auf den Link für den zu ändernden Server.
3. Nehmen Sie Ihre Änderungen auf der entsprechenden Serverseite vor.
4. Klicken Sie auf **Save Changes**.

Konfigurieren einer lokalen Authentifizierungsserverinstanz

Die folgenden Themen werden behandelt:

- „Lokaler Authentifizierungsserver – Übersicht“ auf Seite 225
- „Definieren einer lokalen Authentifizierungsserverinstanz“ auf Seite 225
- „Erstellen lokaler Benutzer“ auf Seite 227
- „Verwalten von Benutzerkonten“ auf Seite 228
- „Delegieren von Benutzerverwaltungsrechten an Endbenutzer“ auf Seite 229

Lokaler Authentifizierungsserver – Übersicht

Im IVE können Sie eine oder mehrere lokale Datenbanken für vom IVE authentifizierte Benutzer erstellen. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie eine Gruppe von temporären Benutzern erstellen möchten. Hinweis: Alle Administratorenkonten werden als lokale Datensätze gespeichert, Administratoren können jedoch über einen externen Server authentifiziert werden. Anweisungen hierfür finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich“ auf Seite 260.

Definieren einer lokalen Authentifizierungsserverinstanz

Wenn Sie eine neue IVE-Serverinstanz definieren, müssen Sie dem Server einen eindeutigen Namen geben und Kennwortoptionen und die Kennwortverwaltung konfigurieren. Mit den Kennwortoptionen haben Sie die Möglichkeit, die Länge des Kennworts, seine Zusammensetzung und Eindeutigkeit zu kontrollieren. Bei Bedarf können Sie Benutzern das Ändern ihres Kennworts ermöglichen, und sie zwingen, Kennwörter nach einer bestimmten Anzahl von Tagen zu ändern. Sie können die Benutzer auch einige Tage vor dem Ablaufdatum des Kennworts auffordern, das Kennwort zu ändern.

So definieren Sie eine lokale Authentifizierungsserverinstanz:

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **IVENew** den Eintrag **Authentication** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie zur Bezeichnung der neuen Serverinstanz einen Namen ein, oder ändern Sie den aktuellen Namen eines vorhandenen Servers.

4. Kennwortoptionen angeben:

   a. Legen Sie unter **Password options** die Mindestzeichenzahl für Kennwörter fest.

   b. Legen Sie die maximale Zeichenzahl für Kennwörter fest (optional). Die maximale Zeichenzahl kann nicht kleiner als die Mindestlänge sein. Für die maximale Zeichenzahl gibt es keine Obergrenze.

HINWEIS: Wenn Sie möchten, dass alle Kennwörter dieselbe Länge haben, legen Sie für die Mindestlänge und für die maximale Länge denselben Wert fest.

   c. Aktivieren Sie das Kontrollkästchen **Password must have at least_digits**, und geben Sie die erforderliche Ziffernzahl für Kennwörter an (optional). Die erforderliche Ziffernzahl darf den Wert der Option **Maximum length** nicht überschreiten.

   d. Aktivieren Sie das Kontrollkästchen **Password must have at least_letters** und geben Sie die erforderliche Buchstabenzahl für Kennwörter an (optional). Die erforderliche Buchstabenzahl darf den Wert der Option **Maximum length** nicht überschreiten. Wenn Sie die vorhergehende Option aktiviert haben, darf die Summe der beiden Optionen den in der Option **Maximum length** angegebenen Wert nicht überschreiten.

   e. Aktivieren Sie das Kontrollkästchen **Password must have mix of UPPERCASE and lowercase letters**, wenn alle Kennwörter sowohl Groß- als auch Kleinbuchstaben enthalten sollen (optional).

HINWEIS: Wenn Sie sowohl Groß- als auch Kleinbuchstaben verlangen, muss die geforderte Buchstabenzahl für Kennwörter mindestens zwei betragen.

   f. Aktivieren Sie das Kontrollkästchen **Password must be different from username**, wenn das Kennwort nicht mit dem Benutzernamen identisch sein darf (optional).

   g. Aktivieren Sie das Kontrollkästchen **New passwords must be different from previous password**, wenn ein neues Kennwort nicht mit dem vorhergehenden Kennwort übereinstimmen darf (optional).

5. Optionen für die Kennwortverwaltung angeben:

   a. Aktivieren Sie unter **Password management** das Kontrollkästchen **Allow users to change their passwords**, wenn die Benutzer die Möglichkeit haben sollen, ihre Kennwörter zu ändern (optional).

   b. Aktivieren Sie das Kontrollkästchen **Force password change after _ days**, und geben Sie die Anzahl an Tagen an, nach denen ein Kennwort abläuft (optional).

HINWEIS: Die Standardeinstellung ist 64 Tage, kann aber beliebig geändert werden.

c. Aktivieren Sie das Kontrollkästchen **Prompt users to change their password _ days before current password expires**, und geben Sie die Zahl der Tage vor dem Ablaufdatum des Kennworts an, wann die Aufforderung der Benutzer zur Kennwortänderung erfolgen soll (optional).

HINWEIS: Die Standardeingabe ist 14 Tage, aber Sie können den Wert ändern und jede Zahl kleiner als die in der vorhergehenden Option angegebene Zahl eintragen.

6. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Users** und **Admin Users** angezeigt.

HINWEIS: Nachdem Sie Kennwortoptionen und Optionen zur Kennwortverwaltung festgelegt haben, müssen Sie angeben, welche Bereiche vom Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwendet werden sollen. Legen Sie mit der Option **Enable Password Management** auf der Seite **Administrators/Users > Authentication >** *Bereich* **> Authentication Policy > Password** fest, ob der Bereich die Kennwortverwaltungseinstellungen der lokalen Authentifizierungsserverinstanz erbt. Informationen über das Aktivieren der Kennwortverwaltung finden Sie unter „Angeben einer Kennwortlängeneinschränkung“ auf Seite 422.

Erstellen lokaler Benutzer

Wenn Sie eine lokale Authentifizierungsserverinstanz erstellen, müssen Sie für diese Datenbank Datensätze für lokale Benutzer definieren. Lokale Benutzerdatensätze bestehen aus einem Benutzernamen, dem vollständigen Namen und dem Kennwort des Benutzers. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie schnell eine Gruppe von temporären Benutzern erstellen möchten.

So erstellen Sie lokale Benutzerdatensätze für einen lokalen Authentifizierungsserver:

1. Führen Sie in der Webkonsole einen der folgenden Vorgänge aus:

   - Wählen Sie **Signing In > AAA Servers** aus, klicken Sie auf die IVE-Datenbank, der Sie ein Benutzerkonto hinzufügen möchten, wählen Sie die Registerkarte **Users** aus, und klicken Sie dann auf **New**.

   - Wählen Sie **Users > New User** aus.

2. Geben Sie einen Benutzernamen ein.

HINWEIS:

- In Benutzernamen darf die Zeichenkombination „ ~ ~ “ nicht enthalten sein.

- Wenn Sie den Benutzernamen eines Benutzers nach dem Erstellen seines Kontos ändern möchten, müssen Sie ein neues Konto erstellen.

3. Geben Sie den vollständigen Namen des Benutzers ein.

4. Geben Sie das Kennwort ein, und bestätigen Sie es.

HINWEIS: Das Kennwort muss den für die zugehörige lokale Authentifizierungsserverinstanz definierten Kennwortoptionen entsprechen.

5. Aktivieren Sie das Kontrollkästchen **Require user to change password at next sign in**, wenn der Benutzer bei der ersten Anmeldung sein Kennwort ändern soll.

6. (Nur auf der Seite **Users > New User**) Wählen Sie aus der Liste **Authenticate Using** die IVE-Datenbank aus, der Sie ein Benutzerkonto hinzufügen möchten.

7. Klicken Sie auf **Save Changes**. Der Benutzerdatensatz wird der IVE-Datenbank hinzugefügt.

Verwalten von Benutzerkonten

So verwalten Sie ein lokales Benutzerkonto

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.

2. Klicken Sie in der Liste **Authentication/Authorization Servers** auf die entsprechende Serververknüpfung.

3. Klicken Sie auf die Registerkarte **Users**.

4. Führen Sie eine der folgenden Aufgaben durch:

   - Geben Sie im Feld **Show Users Named** einen Benutzernamen ein, und klicken Sie auf **Update**, um nach einem bestimmten Benutzer zu suchen.

     Sie können auch ein Sternchen (*) als Platzhalter verwenden, das für eine beliebige Anzahl von Zeichen steht (null, eins oder mehrere). Wenn Sie z. B. nach allen Benutzernamen suchen möchten, die die Buchstaben jo enthalten, geben Sie im Feld **Show users named** die Zeichenfolge *jo* ein. Bei der Suche wird die Groß- und Kleinschreibung berücksichtigt. Wenn Sie wieder die gesamte Liste der Gruppenkonten anzeigen möchten, geben Sie ein Sternchen (*) ein, oder löschen Sie den Feldinhalt, und klicken Sie dann auf **Update**.

   - Geben Sie im Feld **Show N users** eine Zahl ein, und klicken Sie auf **Update**, um die Anzahl von Benutzern anzugeben, die auf der Seite angezeigt werden.

   - Aktivieren Sie das Kontrollkästchen neben den jeweiligen Benutzern, und klicken Sie anschließend auf **Delete**, um deren IVE-Sitzungen zu beenden.

Delegieren von Benutzerverwaltungsrechten an Endbenutzer

Benutzeradministratoren können lokale IVE-Authentifizierungsserver verwalten. Benutzeradministratoren können keine Bereiche oder Rollenzuordnungen verwalten. Daher wird die Aktivierung der Funktion „User Admin“ nur dann empfohlen, wenn die Rollenzuordnungsregeln des Authentifizierungsbereichs es nicht zugeordneten Benutzern (*) erlauben, sich am IVE anzumelden, sodass der Benutzeradministrator neue Benutzer ohne Eingreifen des Administrators hinzufügen kann. (Wenn die Rollenzuordnungen automatisch erfolgen, können Benutzeradministratoren die neuen Benutzer ohne Hilfe des Administrators manuell einer Rolle zuordnen.)

So delegieren Sie Benutzerverwaltungsrechte an einen Endbenutzer:

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.

2. Wählen Sie die lokale Authentifizierungsserverinstanz aus, die vom Benutzeradministrator verwaltet werden soll, und klicken Sie dann auf die Registerkarte **Admin Users**.

HINWEIS: Benutzeradministratoren können nur lokale Authentifizierungsserver verwalten.

---

3. Geben Sie den **Username** des Benutzers ein, der Konten für den ausgewählten Authentifizierungsserver verwalten soll. Dieser Benutzer muss auf dem Server, den er verwaltet, nicht als lokaler Benutzer hinzugefügt werden.

HINWEIS: Achten Sie bei der Eingabe des Benutzernamens des Benutzeradministrators auf die exakte Zeichenfolge. Diese muss genau übereinstimmen.

---

4. Wählen Sie den **Authentication Realm** aus, dem der Benutzeradministrator zugeordnet wird, wenn er sich am IVE anmeldet.

5. Klicken Sie auf **Add**. Das IVE fügt den neuen Benutzeradministrator der Liste **User Admins** im folgenden Format hinzu: Benutzername@Servername.

6. Wenn der angegebene Benutzeradministrator mehreren Bereichen zugeordnet ist, wiederholen Sie ggf. die Schritte 3 bis 5, sodass der Benutzer den Server unabhängig von dem Konto verwalten kann, über das er sich beim IVE anmeldet.

7. Um dem Benutzer die Verwaltungsrechte wieder zu entziehen, wählen Sie in der Liste **User Admins** den entsprechenden Namen aus, und klicken Sie auf **Remove**.

HINWEIS: Informationen zum Verwalten von Benutzern über die Startseite des sicheren Gateways finden Sie in der Hilfe für den Endbenutzer im Thema „Hinzufügen und Ändern von Benutzern“. Die Hilfe steht dem Endbenutzer nach der Anmeldung am IVE zur Verfügung.

Konfigurieren einer LDAP-Serverinstanz

Die Seite **LDAP-System** enthält die folgenden Registerkarten:

- „Registerkarte „Einstellungen““ auf Seite 230 – Diese Registerkarte dient zum Definieren von einer LDAP-Serverinstanz.
- „Registerkarte „Users““ auf Seite 232 – Diese Registerkarte dient zum Überwachen und Löschen von aktiven Benutzersitzungen.

Registerkarte „Einstellungen“

Das IVE unterstützt zwei LDAP-spezifische Authentifizierungsoptionen:

- **Unencrypted** – Das IVE sendet den Benutzernamen und das Kennwort in einfachem Klartext an den LDAP-Verzeichnisdienst.
- **LDAPS** – Das IVE verschlüsselt die Daten in der LDAP-Authentifizierungssitzung mit dem SSL-Protokoll (Secure Socket Layer), bevor sie an den LDAP-Verzeichnisdienst gesendet werden.

Festlegen einer LDAP-Serverinstanz

So definieren Sie eine LDAP-Serverinstanz:

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **LDAP Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des LDAP-Servers an, der vom IVE zur Überprüfung von Benutzern verwendet wird.
5. Geben Sie den Port an, den der LDAP-Server überwacht. Dies ist bei Verwendung einer unverschlüsselten Verbindung normalerweise Port 389 und bei Verwendung von SSL Port 636.

6. Geben Sie Parameter für LDAP-Sicherungsserver an (optional). Das IVE verwendet die angegebenen Server für die Failover-Verarbeitung. Jede Authentifizierungsanforderung wird zuerst an den primären LDAP-Server und dann an den oder die angegebenen Sicherungsserver weitergeleitet, falls der primäre Server nicht erreichbar ist.

HINWEIS: LDAP-Sicherungsserver müssen dieselbe Version wie der primäre LDAP-Server aufweisen. Darüber hinaus empfiehlt es sich, nicht den Hostnamen, sondern die IP-Adresse eines LDAP-Sicherungsservers anzugeben, denn dadurch kann die Failover-Verarbeitung beschleunigt werden, da der Hostname nicht in eine IP-Adresse aufgelöst werden muss.

---

7. Geben Sie den Typ des LDAP-Servers an, über den Sie Benutzer authentifizieren möchten.

8. Geben Sie an, ob die Verbindung zwischen dem IVE und dem LDAP-Verzeichnisdienst unverschlüsselt bleiben oder ob SSL (LDAPs) verwendet werden soll.

9. Legen Sie fest, wie lange das IVE auf eine Verbindung mit dem primären LDAP-Server warten soll, und geben Sie dann nacheinander die Wartezeit für jeden Backup-LDAP-Server an.

10. Legen Sie fest, wie lange das IVE auf Suchergebnisse von einem verbundenen LDAP-Server warten soll.

11. Klicken Sie auf **Test Connection**, um die Verbindung zwischen der IVE-Appliance und den angegebenen LDAP-Servern zu überprüfen. (Dies ist optional.)

12. Aktivieren Sie das Kontrollkästchen **Authentication required to search LDAP**, wenn das IVE für eine Suche eine Authentifizierung durch das LDAP-Verzeichnis durchführen muss. Geben Sie anschließend einen Administrator-DN und ein Kennwort ein. Beispiel:

    CN=Administrator,CN=Users,DC=eng,DC=Juniper,DC=com

13. Geben Sie unter **Finding user entries** Folgendes an:

    - **Base DN**, von dem an nach Benutzereinträgen gesucht werden soll. Beispiel:

      DC=eng,DC=Juniper,DC=com

    - **Filter**, wenn die Suche eingegrenzt werden soll. Beispiel:

      samAccountname=<username> oder cn=<username>

      - Fügen Sie zur Verwendung des Benutzernamens, der auf der Anmeldeseite für die Suche eingegeben wurde, im Filter die Zeichenfolge <username> ein.

      - Geben Sie einen Filter an, der keinen (0) oder einen (1) Benutzer-DN pro Benutzer zurückgibt. Falls mehrere DNs zurückgegeben werden, verwendet das IVE den ersten zurückgegebenen DN.

14. Das IVE unterstützt sowohl statische als auch dynamische Gruppen. Zum Aktivieren des Gruppenlookups müssen Sie angeben, wie das IVE den LDAP-Server nach einer Gruppe durchsuchen soll. Geben Sie unter **Determining group membership** Folgendes an:

    - **Base DN**, ab dem die Suche nach Benutzergruppen beginnen soll.
    - **Filter**, wenn die Suche nach einer Benutzergruppe optimiert werden soll.
    - **Member Attribute**, um alle Mitglieder einer statischen Gruppe zu identifizieren. Beispiel:

      member
      uniquemember (iPlanet-spezifisch)

    - **Query Attribute**, um eine LDAP-Abfrage anzugeben, die die Mitglieder einer dynamischen Gruppe zurückgibt. Beispiel:

      memberURL

    - **Nested Group Level**, um anzugeben, wie viele Ebenen innerhalb einer Gruppe nach dem Benutzer durchsucht werden sollen. Beachten Sie Folgendes: Je höher die Anzahl, desto länger die Abfragezeit. Daher wird empfohlen, für die Suche nicht mehr als zwei Ebenen anzugeben.

15. Wählen Sie unter **Bind Options** Folgendes aus:

    - **Simple bind**, um die Anmeldeinformationen eines Benutzers im Klartext (unverschlüsselt) an den LDAP-Verzeichnisdienst zu senden.
    - **StartTLS bind**, um die Anmeldeinformationen eines Benutzers über das TLS-Protokoll (Transport Layer Security) zu verschlüsseln, bevor das IVE die Daten an den LDAP-Verzeichnisdienst sendet.

16. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.

17. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll. Weitere Informationen finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich“ auf Seite 260.

Registerkarte „Users“

Anzeigen und Löschen von aktiven Benutzersitzungen

Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 254.

Konfigurieren einer NIS-Serverinstanz

Die folgenden Themen werden behandelt:

- „Authentifizieren von Benutzern mit einem NIS-Server“ auf Seite 233
- „Festlegen einer NIS-Serverinstanz“ auf Seite 233

Authentifizieren von Benutzern mit einem NIS-Server

Beim Authentifizieren von Benutzern mit einem UNIX/NIS-Server überprüft der IVE, ob der auf der Anmeldeseite eingegebene Benutzername und das Kennwort einem gültigen Paar aus Benutzer-ID und Kennwort auf dem NIS-Server entsprechen. Beachten Sie, dass der an das IVE gesendete Benutzername keine zwei aufeinander folgenden Tilden (~ ~) enthalten darf.

HINWEIS: Sie können NIS-Authentifizierung nur mit dem IVE verwenden, wenn die Kennwörter auf dem NIS-Server im Crypt- oder MD5-Format gespeichert sind. Außerdem können Sie dem IVE nur eine NIS-Serverkonfiguration hinzufügen, mit der jedoch eine beliebige Anzahl von Bereichen authentifiziert werden können.

Festlegen einer NIS-Serverinstanz

So definieren Sie eine NIS-Serverinstanz:

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **NIS Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des NIS-Servers an.
5. Geben Sie den Domänennamen für den NIS-Server an.
6. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
7. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll. Weitere Informationen finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich“ auf Seite 260.

HINWEIS: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 254.

Konfigurieren einer ACE/Serverinstanz

Die folgenden Themen werden behandelt:

- „ACE/Server – Übersicht“ auf Seite 234
- „Festlegen einer ACE/Serverinstanz“ auf Seite 235
- „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 236

ACE/Server – Übersicht

Bei der Authentifizierung von Benutzern mit einem RSA ACE/Server ruft der Benutzer die IVE-Standardanmeldeseite auf und gibt dann den Benutzernamen und das Kennwort ein (bestehend aus der Kombination von PIN und dem aktuellen Wert des RSA SecurID-Hardwaretokens). Das IVE leitet diese Anmeldeinformationen des Benutzers dann an ACE/Server weiter.

Wenn der ACE/Server den Benutzer authentifiziert, wird der Zugriff auf das IVE gewährt. Andernfalls führt der ACE/Server folgende Aktionen aus:

- Der Benutzerzugriff auf das System wird verweigert, wenn die Anmeldedaten des Benutzers nicht erkannt werden.
- Der Benutzer wird aufgefordert, eine neue PIN zu generieren (New PIN-Modus), wenn er sich erstmals am IVE anmeldet. (Dem Benutzer werden je nach verwendetem Anmeldeverfahren unterschiedliche Aufforderungen angezeigt. Bei Anmeldung mit dem SoftID-Plug-In werden die RSA-Aufforderungen zum Erstellen einer neuen PIN angezeigt. Andernfalls werden die IVE-Aufforderungen angezeigt.)
- Der Benutzer wird aufgefordert, das nächste Token einzugeben (Next Token-Modus), wenn das vom Benutzer eingegebene Token nicht mit dem vom ACE/Server erwarteten Token übereinstimmt. (Der Next Token-Modus ist für Benutzer transparent, die sich mit dem SoftID-Token anmelden. Die RSA SecurID-Software übergibt das Token über die IVE und ohne Benutzerinteraktion an ACE/Server.)
- Der Benutzer wird an die IVE-Standardanmeldeseite umgeleitet (nur SoftID), wenn er versucht, sich auf einem Computer ohne installierte SecurID-Software an der Seite **RSA SecurID Authentication** anzumelden.

Wenn der Benutzer die neue PIN oder das nächste Token eingibt (je nach Modus), bleiben drei Minuten für die Eingabe der erforderlichen Informationen. Danach bricht das IVE die Transaktion ab und fordert den Benutzer zur erneuten Eingabe der Anmeldeinformationen auf.

Das IVE kann bis zu 200 ACE/Server-Transaktionen gleichzeitig verarbeiten. Eine Transaktion dauert nur so lange wie die Authentifizierung bei ACE/Server. Wenn sich ein Benutzer z. B. am IVE anmeldet, wird die ACE/Server-Transaktion beim Senden der Anforderung durch den Benutzer initiiert. Die Transaktion wird beendet, sobald ACE/Server die Verarbeitung der Anforderung beendet hat. Der Benutzer kann mit der IVE-Sitzung fortfahren, obwohl die ACE/Server-Transaktion beendet wurde.

Das IVE unterstützt die folgenden ACE/Server-Features: New PIN-Modus, Next Token-Modus, DES/SDI-Verschlüsselung, AES-Verschlüsselung, Unterstützung untergeordneter ACE/Server, Namenssperrungen und Clustering. Das IVE unterstützt über das RADIUS-Protokoll auch die New PIN- und Next Token-Modi von RSA SecurID.

HINWEIS: Wegen der Einschränkungen der ACE/Server-Bibliothek unter UNIX können Sie u. U. nur eine ACE/Server-Konfiguration festlegen. Informationen zum Erzeugen einer ACE/Agent-Konfigurationsdatei für die IVE auf dem ACE-Server finden Sie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 236.

Festlegen einer ACE/Serverinstanz

HINWEIS: Sie können nur eine ACE/Serverinstanz hinzufügen.

So definieren Sie einen ACE/Server:

1. Erzeugen Sie eine ACE/Agent-Konfigurationsdatei (sdconf.rec) für das IVE auf dem ACE-Server. Weitere Informationen finden Sie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 236.

2. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.

3. Führen Sie einen der folgenden Vorgänge aus:

   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **ACE Server** aus, und klicken Sie dann auf **New Server**.

   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.

4. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.

5. Geben Sie im Feld **ACE Port** einen Standardport an. Das IVE verwendet diese Einstellung nur, wenn in der Datei sdconf.rec kein Port angegeben ist.

6. Importieren Sie die RSA ACE/Agent-Konfigurationsdatei. Aktualisieren Sie diese Datei im IVE unbedingt bei jeder Änderung an der Quelldatei. Wenn Sie die Instanzdatei aus dem IVE löschen, müssen Sie ebenfalls zur Konfigurationsverwaltungsanwendung für ACE-Server wechseln, wie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 236 beschrieben, und das Kontrollkästchen **Sent Node Secret** deaktivieren.

7. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.

8. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll. Weitere Informationen finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich“ auf Seite 260.

HINWEIS: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 254.

Generieren einer ACE/Agent-Konfigurationsdatei

Wenn Sie ACE/Server für die Authentifizierung verwenden, müssen Sie auf dem ACE-Server eine ACE/Agent-Konfigurationsdatei (sdconf.rec) für das IVE generieren.

So generieren Sie eine ACE/Agent-Konfigurationsdatei

1. Starten Sie die Konfigurationsverwaltungsanwendung für ACE-Server, und klicken Sie auf **Agent Host**.
2. Klicken Sie auf **Add Agent Host**.
3. Geben Sie unter **Name** einen Namen für den IVE-Agenten ein.
4. Geben Sie unter **Network Address** die IP-Adresse des IVE ein.
5. Geben Sie eine auf dem ACE-Server konfigurierte **Site** an.
6. Wählen Sie als **Agent Type** den Typ **Communication Server** aus.
7. Wählen Sie als **Encryption Type** den Typ **DES** aus.
8. Vergewissern Sie sich, dass **Sent Node Secret** (beim Erstellen eines neuen Agenten) deaktiviert ist.

   Wenn der ACE-Server eine vom IVE gesendete Anforderung erfolgreich authentifiziert, wählt der ACE-Server **Sent Node Secret** aus. Wenn der ACE-Server später einen neuen Knotenschlüssel an das IVE senden soll, gehen Sie bei der nächsten Authentifizierungsanforderung folgendermaßen vor:

   a. Deaktivieren Sie das Kontrollkästchen **Sent Node Secret**, indem Sie auf dieses klicken.

   b. Melden Sie sich an der IVE-Webkonsole an, und wählen Sie **Signing In > AAA Servers**.

   c. Klicken Sie in der Liste **Authentication/Authorization Servers** auf den Namen des entsprechenden ACE-Servers.

   d. Aktivieren Sie unter **Node Verification File** das entsprechende Kontrollkästchen aus, und klicken Sie auf **Delete**. Durch diese Schritte wird sichergestellt, dass der IVE-Server und der ACE-Server synchronisiert sind. Entsprechend sollten Sie auf dem ACE-Server das Kontrollkästchen **Sent Node Secret** deaktivieren, wenn Sie die Überprüfungsdatei aus dem IVE löschen.

9. Klicken Sie auf **Assign Acting Servers**, und wählen Sie den ACE-Server aus.

10. Klicken Sie auf **Generate Config File**. Wenn Sie den ACE-Server zum IVE hinzufügen, wird diese Konfigurationsdatei importiert.

Konfigurieren einer RADIUS-Serverinstanz

Die folgenden Themen werden behandelt:

- „RADIUS-Server – Übersicht“ auf Seite 238
- „Unterstützte Authentifizierungsschemas“ auf Seite 238
- „Optionen für RADIUS-Benutzer“ auf Seite 239
- „Aktivieren der RADIUS-Kontoführung“ auf Seite 240
- „Konfigurieren des IVE für die Zusammenarbeit mit einem RADIUS-Server“ auf Seite 242

RADIUS-Server – Übersicht

Ein RADIUS-Server (Remote Authentication Dial-In User Service) ermöglicht es Ihnen, die Authentifizierung und Kontoführung für Remotebenutzer zu zentralisieren. Beim Authentifizieren von IVE-Benutzern mit einem RADIUS-Server müssen Sie den Server so konfigurieren, dass das IVE als Client erkannt wird. Außerdem müssen Sie für den RADIUS-Server einen gemeinsamen geheimen Schlüssel zur Verwendung bei der Authentifizierung der Clientanforderung angeben.

Unterstützte Authentifizierungsschemas

Der IVE unterstützt die RADIUS-Standardauthentifizierungsschemas. Zu diesen gehören folgende:

- Access-Request
- Access-Accept
- Access-Reject
- Access-Challenge

Der IVE unterstützt auch RSA ACE/Server unter Verwendung des RADIUS-Protokolls und eines SecurID-Tokens (erhältlich von Security Dynamics). Wenn Sie für die Authentifizierung von Benutzern SecurID verwenden, müssen die Benutzer ihre Benutzer-ID und die Kombination aus PIN und dem Tokenwert angeben.

Beim Festlegen eines RADIUS-Servers gibt das IVE Administratoren die Möglichkeit, entweder hart codierte Anfrageausdrücke (Standard) zu verwenden, die Defender 4.0 und einige RADIUS-Server-Implementierungen unterstützen (wie z. B. Steelbelted-RADIUS und RSA RADIUS), oder benutzerdefinierte Anfrageausdrücke einzugeben, die dem IVE ermöglichen, mit vielen verschiedenen RADIUS-Implementierungen und neuen Versionen vom RADIUS-Server, wie z. B. Defender 5.0, zu arbeiten. Das IVE sucht die Antwort im Access-Challenge-Paket vom Server und gibt eine Anfrage nach dem nächsten Token, einer neuen PIN oder einem generischen Kenncode an den Benutzer aus.

Optionen für RADIUS-Benutzer

Für den Benutzer unterscheidet sich das Authentifizierungsverhalten abhängig davon, ob Sie einen PassGo Defender RADIUS-Server oder die CASQUE-Authentifizierung verwenden.

Verwenden eines PassGo Defender RADIUS-Servers

Wenn Sie einen PassGo Defender-RADIUS-Server verwenden, erfolgt die Benutzeranmeldung folgendermaßen:

1. Der Benutzer meldet sich beim IVE mit einem Benutzernamen und einem Kennwort an. Das IVE leitet diese Anmeldeinformationen an Defender weiter.
2. Defender sendet eine eindeutige Anfragezeichenfolge an das IVE, und im IVE wird diese Anfragezeichenfolge dem Benutzer angezeigt.
3. Der Benutzer gibt die Anfragezeichenfolge in einem Defender-Token ein, und das Token erzeugt eine Antwortzeichenfolge.
4. Der Benutzer gibt die Antwortzeichenfolge im IVE ein und klickt auf **Sign In**.

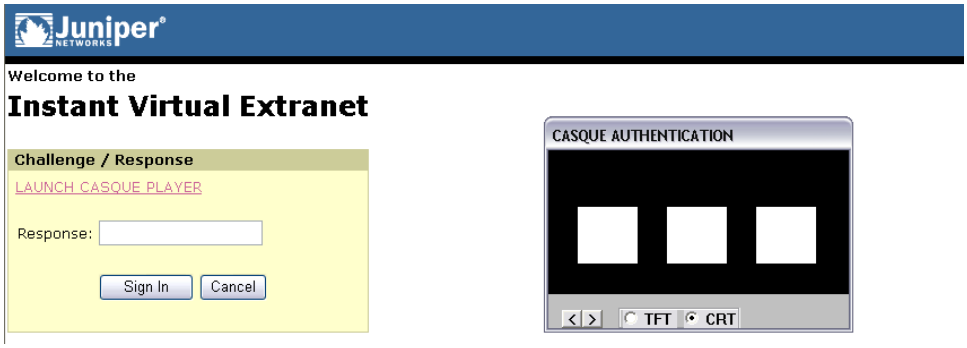
Verwenden der CASQUE-Authentifizierung

Die CASQUE-Authentifizierung verwendet einen tokenbasierten Anfrage/Antwort-Authentifizierungsmechanismus, bei dem ein auf dem Clientsystem installierter CASQUE-Player zur Anwendung kommt. Nachdem der RADIUS-Server mit der CASQUE-Authentifizierung konfiguriert wurde, gibt er eine Anfrage mit einer auf den benutzerdefinierten Anfrageausdruck passenden Antwort aus (:([0-9a-zA-Z/+=]+):). Das IVE erstellt dann eine zwischengeschaltete Seite, die den auf dem System des Benutzers installierten CASQUE-Player automatisch startet.

HINWEIS: Sollte der CASQUE-Player nicht automatisch gestartet werden, klicken Sie auf die Verknüpfung **Launch CASQUE Player**.

Die Benutzer müssen dann ihre CASQUE Optical Responder-Tokens zur Erstellung des entsprechenden Kenncodes verwenden, den Kenncode im Feld **Response** eingeben und auf **Sign In** klicken.

Abbildung 30: Anfrage/Antwort-Seite für CASQUE-Authentifizierung mit CASQUE-Player



Aktivieren der RADIUS-Kontoführung

Das Secure Access 700 kann so konfiguriert werden, dass es Meldungen über den Sitzungsstart und das Sitzungsende an einen RADIUS-Kontoführungsserver sendet. Das IVE erkennt zwei Kategorien von Network Connect-Sitzungen – Benutzersitzungen und Subsitzungen. Eine Benutzersitzung kann mehrere Subsitzungen enthalten.

Das IVE sendet eine Meldung über den Benutzersitzungsstart, nachdem sich der Benutzer erfolgreich angemeldet hat und ihm vom IVE eine Rolle zugeordnet wurde. Das IVE sendet eine Meldung über den Subsitzungsstart, wenn die Subsitzung aktiv wird. Das IVE sendet eine Meldung über das Subsitzungsende, wenn der Benutzer explizit die Beendigung einer Subsitzung anfordert oder die Benutzersitzung beendet wird.

Wenn eine Benutzersitzung beendet wird, sendet das IVE eine Meldung über das Benutzersitzungsende an den Kontoführungsserver. Eine Benutzersitzung wird in den folgenden Fällen beendet:

- Der Benutzer meldet sich manuell vom IVE ab.
- Die Verbindung des Benutzers mit dem IVE läuft aufgrund von Inaktivität oder einer Überschreitung der maximalen Sitzungsdauer ab.
- Dem Benutzer wird der Zugriff aufgrund von Host Checker- oder Cache Cleaner-Einschränkungen auf Rollenebene verweigert.
- Die Verbindung des Benutzers mit dem IVE wird manuell von einem Administrator oder aufgrund einer dynamischen Richtlinienauswertung getrennt.

Das IVE sendet auch Beendigungsmeldungen für alle aktiven Subsitzungen. Die Beendigungsmeldungen für die Subsitzungen werden vor den Beendigungsmeldungen für die Benutzersitzung gesendet.

HINWEIS: Wenn Ihre Benutzer an einem IVE-Cluster angemeldet sind, wird in den Kontoführungsmeldungen von RADUIS u. U. angezeigt, dass sich die Benutzer an einem Knoten anmelden und an einem anderen abmelden.

Die folgenden drei Tabellen beschreiben die gemeinsamen Attribute von Start- und Beendigungsmeldungen, die speziellen Attribute von Startmeldungen und die speziellen Attribute von Beendigungsmeldungen.

Tabelle 9: Attribute von Start- und Beendigungsmeldungen

Attribut	Beschreibung
User-Name (1)	Während der RADIUS-Serverkonfiguration vom IVE-Administrator festgelegte Zeichenfolge
NAS-IP-Address (4)	IP-Adresse des IVE
NAS-Port (5)	Das IVE setzt dieses Attribut auf 0, wenn sich der Benutzer an einem internen Port angemeldet hat, und im Fall eines externen Ports auf 1.

Tabelle 9: Attribute von Start- und Beendigungsmeldungen (Fortsetzung)

Attribut	Beschreibung
Framed-IP-Address (8)	Quell-IP-Adresse des Benutzers
NAS-Identifier (32)	Konfigurierter Name für den IVE-Client unter der RADIUS-Serverkonfiguration
Acct-Status-Type (40)	Das IVE setzt dieses Attribut für eine Startmeldung in einer Benutzer- oder Subsitzung auf 1 und für eine Beendigungsmeldung auf 2.
Acct-Session-Id (44)	Eindeutige Kontoführungs-ID, die Start- und Beendigungsmeldungen mit einer Benutzer- oder Subsitzung abgleicht
Acct-Multi-Session-Id (50)	Eindeutige Kontoführungs-ID, mit der mehrere verwandte Sitzungen verknüpft werden können. Jeder verknüpften Sitzung muss eine eindeutige „Acct-Session-Id“ und die gleiche „Acct-Multi-Session-Id“ zugewiesen sein.
Acct-Link-Count (51)	Die Anzahl von Links in einer Sitzung mit mehreren Links zu dem Zeitpunkt, zu dem das IVE den Kontoführungsdatensatz erstellt

Tabelle 10: Startattribute

Attribut	Beschreibung
Acct-Authentic (45)	Das IVE stellt dieses Attribut wie folgt ein: ■ RADIUS – wenn der Benutzer mit einem RADIUS-Server authentifiziert wird. ■ Local – wenn der Benutzer mit einem lokalen IVE-Authentifizierungsserver authentifiziert wird. ■ Remote – für allen anderen Authentifizierungsmethoden.

Tabelle 11: Beendigungsattribute

Attribut	Beschreibung
Acct-Session-Time (46)	Dauer der Benutzer- oder Subsitzung
Acct-Terminate-Cause (49)	Das IVE verwendet einen der folgenden Werte, um das Ereignis anzugeben, das zur Beendigung einer Benutzer- oder Subsitzung geführt hat: ■ User Request (1) – Manuelle Abmeldung des Benutzers ■ Idle Timeout (4) – Leerlaufzeitlimit für Benutzer überschritten ■ Session Timeout (5) – Sitzungszeitlimit für Benutzer überschritten ■ Admin Reset (6) – Benutzer zum Beenden der Seite **Active Users** gezwungen

Sie können eine Benutzersitzung und die in ihr enthaltenen Subsitzungen anhand der Attribute „Acct-Session-Id“ „und Acct-Multi-Session-Id“ unterscheiden. In einer Benutzersitzung sind diese beiden Attribute identisch. In einer Subsitzung ist das Attribut „Acct-Multi-Session-Id“ mit dem Attribut für die übergeordnete Benutzersitzung identisch, und das Secure Access 700 kennzeichnet die Subsitzung durch eines der „NC“-Suffixe im Attribut „Acct-Session-Id“.

Konfigurieren des IVE für die Zusammenarbeit mit einem RADIUS-Server

Dieser Abschnitt enthält die folgenden Anweisungen zur Konfiguration des IVE und des RADIUS-Servers für die Zusammenarbeit:

- „Festlegen einer IVE-RADIUS-Serverinstanz“ auf Seite 242
- „Konfigurieren des RADIUS-Servers für die Erkennung des IVE“ auf Seite 244

Festlegen einer IVE-RADIUS-Serverinstanz

So konfigurieren Sie eine Verbindung zum RADIUS-Server auf dem IVE:

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **Radius Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Führen Sie im oberen Bereich der Seite **Radius Server** Folgendes aus:
   a. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
   b. Geben Sie den Namen oder die IP-Adresse des RADIUS-Servers an.
   c. Geben Sie den Wert für den Authentifizierungsport für den RADIUS-Server ein. Normalerweise ist dies Port 1812, einige Legacyserver könnten jedoch auch Port 1645 verwenden.
   d. Geben Sie eine Zeichenfolge für den gemeinsamen geheimen Schlüssel ein. Sie müssen diese Zeichenfolge auch eingeben, wenn Sie den RADIUS-Server für die Erkennung des IVE-Geräts als Client konfigurieren.
   e. Geben Sie den Wert für den Kontoführungsport für den RADIUS-Server ein. Normalerweise ist dies Port 1813, einige Legacyserver könnten jedoch auch Port 1646 verwenden.
   f. Geben Sie die Zeitspanne ein, für die das IVE auf eine Antwort vom RADIUS-Server bis zur Zeitüberschreitung für die Verbindung warten soll.
   g. Geben Sie die Anzahl der weiteren Verbindungsversuche ein, die das IVE nach dem ersten fehlgeschlagenen Versuch ausführen soll.
   h. Aktivieren Sie das Kontrollkästchen **Users authenticate using tokens or one-time passwords**, wenn Sie das vom Benutzer eingegebene Kennwort nicht an andere SSO-fähige Annwendungen übermitteln wollen. In der Regel sollten Sie diese Option auswählen, wenn Benutzer Einmal-Kennwörter im IVE eingeben.

4. Geben Sie im Abschnitt **Backup Server** einen sekundären RADIUS-Server an, der vom IVE verwendet werden soll, wenn der in dieser Instanz definierte primäre Server nicht erreichbar ist. Geben Sie für den sekundären Server folgende Angaben ein:

   a. Name oder IP-Adresse

   b. Authentifizierungsport

   c. Gemeinsamer geheimer Schlüssel

   d. Kontoführungsport

5. Wenn Sie das Benutzeraufkommen für IVE mithilfe dieser Instanz des RADIUS-Servers ermitteln wollen, geben Sie im Abschnitt **Radius Accounting** folgende Informationen ein:

   a. Geben Sie in das Feld **NAS-Identifier** den Namen des IVE Network Access Server (NAS)-Client ein, der mit dem RADIUS-Server kommuniziert. Wenn Sie dieses Feld leer lassen, verwendet das IVE den Wert, der im Feld **Hostname** auf der Seite **System > Network > Overview** in der Webkonsole festgelegt wurde. Sollte in diesem Feld kein Wert festgelegt sein, verwendet das IVE den Wert „Juniper IVE".

   b. Geben Sie im Feld **User-Name** die Benutzerinformationen ein, die vom IVE an den RADIUS-Kontoführungsserver gesendet werden sollen. Zu den zutreffenden Variablen zählen die nach der Anmeldung und Rollenzuordnung des Benutzers festgelegten Variablen. Die Standardvariablen für dieses Feld lauten:

      - <username> protokolliert den IVE-Benutzernamen des Benutzers auf dem Kontoführungsserver.
      - <REALM> protokolliert den IVE-Bereich des Benutzers auf dem Kontoführungsserver.
      - <ROLE> protokolliert die IVE-Rolle des Benutzers auf dem Kontoführungsserver. Wird der Benutzer mehreren Rollen zugeordnet, trennt das IVE die Rollen durch Kommas.

6. Hinzufügen eines benutzerdefinierten Anfrageausdrucks (optional). Es werden grundsätzlich drei Typen von Anfrageausdrücken unterschieden, wobei jeder automatisch auf die voreingestellten Standardeinstellungen gesetzt wird. Mit der benutzerdefinierten Option kann der Administrator das jeweilige Zeichenfolgemuster auf einen der drei Typen abgleichen. Um einen benutzerdefinierten Ausdruck hinzuzufügen, wählen Sie das Optionsfeld **Custom** unter dem entsprechenden Anfrageausdrucktyp, und fügen Sie im entsprechenden Textfeld einen benutzerdefinierten Ausdruck hinzu.

HINWEIS: Geben Sie bei Verwendung der CASQUE-Authentifizierung **:([0-9a-zA-Z/+=]+):** als benutzerdefinierten Ausdruck für **Generic Login Challenge Expression** an.

7. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.

8. Geben Sie die Bereiche an, die der Server für die Authentifizierung, Autorisierung oder Kontoführung von Administratoren und Benutzern verwenden soll. Weitere Informationen finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich“ auf Seite 260.

HINWEIS: Informationen zum Überwachen und Löschen der Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 254.

Konfigurieren des RADIUS-Servers für die Erkennung des IVE

Sie müssen den RADIUS-Server durch folgende Angaben so konfigurieren, dass er den IVE-Server erkennt:

- Hostname des IVE.
- Netzwerk-IP-Adresse des IVE.
- Clienttyp des IVE (sofern vorhanden). Wenn diese Option verfügbar ist, wählen Sie „Single Transaction Server“ oder die entsprechende Option.
- Verschlüsselungstyp für die Authentifizierung der Clientkommunikation. Die ausgewählte Option muss mit dem Clienttyp übereinstimmen.
- Gemeinsamer geheimer Schlüssel, der in der Webkonsole auf der Seite **Signing In > AAA Servers > Radius Server** für den RADIUS-Server eingegeben wurde.

Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz

Die folgenden Themen werden behandelt:

- „Active Directory/Windows NT Server – Übersicht“ auf Seite 245
- „Domänenübergreifende Benutzerauthentifizierung“ auf Seite 245
- „Unterstützung der Gruppensuche für Active Directory und NT“ auf Seite 247
- „Definieren einer Active Directory-oder Windows NT-Domänenserverinstanz“ auf Seite 248

Active Directory/Windows NT Server – Übersicht

Wenn die Benutzerauthentifizierung über einen primären NT-Domänencontroller (PDC) oder Active Directory erfolgt, melden sich Benutzer mit dem für den Zugriff auf den eigenen Windows-Desktop verwendeten Benutzernamen und Kennwort am IVE an. Das IVE unterstützt die Windows NT-Authentifizierung und Active Directory mit NTLM- oder Kerberos-Authentifizierung.

Wenn Sie einen systemeigenen Active Directory-Server konfigurieren, können Sie Gruppeninformationen vom Server für die Verwendung in den Rollenzuordnungsregeln eines Bereichs abrufen. In diesem Fall legen Sie den Active Directory-Server als den Authentifizierungsserver des Bereichs fest, und anschließend erstellen Sie eine Rollenzuordnungsregel auf Grundlage der Gruppenmitgliedschaft. Das IVE zeigt alle Gruppen des konfigurierten Domänencontrollers und dessen vertrauenswürdiger Domänen an. Weitere Informationen finden Sie unter „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 261.

HINWEIS:

- Das IVE berücksichtigt Vertrauensstellungen in Active Directory und Windows NT-Umgebungen.
- Das IVE unterstützt lokale und globale Gruppen in der Domäne sowie universelle Gruppen, die in der Active Directory-Gesamtstruktur definiert sind. Unterstützt werden auch lokale und globale Gruppen der Domäne für NT4-Server.
- Das IVE lässt nur Active Directory-Sicherheitsgruppen zu, keine Verteilergruppen. Mit Sicherheitsgruppen können Sie einen Gruppentyp sowohl für das Zuweisen von Berechtigungen als auch für E-Mail-Verteilerlisten verwenden.

Domänenübergreifende Benutzerauthentifizierung

Das IVE ermöglicht die domänenübergreifende Authentifizierung für Active Directory und Windows NT. Das IVE authentifiziert Benutzer in der auf der Seite **Signing In > AAA Servers > New Active Directory / Windows NT** konfigurierten Domäne, Benutzer in untergeordneten Domänen sowie Benutzer in allen Domänen, denen die konfigurierte Domäne vertraut.

Nachdem Sie die Adresse eines Domänencontrollers und eine Standarddomäne in der Active Directory-Serverkonfiguration des IVE festgelegt haben, verwenden Benutzer in der Standarddomäne für die Authentifizierung beim IVE entweder nur ihren Benutzernamen oder den Standarddomänen- und den Benutzernamen im folgenden Format: standarddomaene\benutzername.

Wenn Sie die Authentifizierung für vertrauenswürdige Domänen aktivieren, können Benutzer in vertrauenswürdigen oder untergeordneten Domänen für die Authentifizierung beim IVE den Namen der vertrauenswürdigen bzw. untergeordneten Domäne und den Benutzernamen im folgenden Format verwenden: vertrauensürdigedomaene\benutzername. Durch das Aktivieren der Authentifizierung für vertrauenswürdige Domänen verlängert sich die Antwortzeit des Servers.

Domänenübergreifende Authentifizierung für Windows 2000 und Windows 2003

Das IVE unterstützt die Kerberos-basierte Active Directory-Authentifizierung mit Windows 2000- und Windows 2003-Domänencontrollern. Wenn sich ein Benutzer am IVE anmeldet, erfolgt die Kerberos-Authentifizierung. Dabei versucht das IVE, den Kerberos-Bereichsnamen für den Domänencontroller sowie alle untergeordneten und vertrauenswürdigen Bereiche mithilfe von LDAP-Aufrufen abzurufen.

Als Alternative könnten Sie den Kerberos-Bereichsnamen beim Konfigurieren eines Active Directory-Authentifizierungsservers festlegen, aber diese Methode wird aus folgenden zwei Gründen nicht empfohlen:

- Sie können nur einen Bereichsnamen festlegen. Das IVE kann deshalb keine Authentifizierung durch die untergeordneten oder vertrauenswürdigen Bereiche des von Ihnen festgelegten Bereichs ausführen.
- Wenn Sie den Bereichsnamen falsch eingeben, kann das IVE Benutzer nicht für den korrekten Bereich authentifizieren.

Domänenübergreifende Authentifizierung für Windows NT4

Das IVE unterstützt nicht die Kerberos-basierte Authentifizierung in Windows NT4-Domänencontrollern. Anstelle von Kerberos wird die NTLM-Authentifizierung verwendet.

HINWEIS: Für die Benutzerauthentifizierung stellt das IVE eine Verbindung mit dem Standard-Domänencontrollerserver her, wobei für den Computernamen das Format <IVE-IPaddress> verwendet wird.

HINWEIS: Vergewissern Sie sich bei Änderungen an der DNS-Datei, dass die untergeordneten und vertrauenswürdigen Domänen vom IVE mittels WINS, DNS oder den Hostdateien aufgelöst werden.

Benutzernormalisierung für NT

Zur Unterstützung der domänenübergreifenden Authentifizierung verwendet das IVE „normalisierte“ NT-Anmeldedaten für die Authentifizierung über einen Active Directory- oder NT4-Domänencontroller. Zu den normalisierten NT-Anmeldedaten gehören der Domänenname und der Benutzername: domaene\benutzername. Unabhängig davon, wie sich der Benutzer am IVE anmeldet – mit dem Benutzernamen oder dem Format „domaene\benutzername“ –, das IVE verarbeitet den Benutzernamen immer im Format domaene\benutzername.

Wenn ein Benutzer versucht, sich nur mit dem Benutzernamen zu authentifizieren, normalisiert das IVE die NT-Anmeldedaten immer im Format standarddomaene\benutzername. Die Authentifizierung ist nur erfolgreich, wenn der Benutzer Mitglied in der Standarddomäne ist.

Für einen Benutzer, der sich mit dem Format domaene\benutzername am IVE anmeldet, versucht das IVE immer, den Benutzer als Mitglied der von ihm angegebenen Domäne zu authentifizieren. Die Authentifizierung ist nur erfolgreich, wenn die vom Benutzer angegebene Domäne eine vertrauenswürdige oder untergeordnete Domäne der Standarddomäne ist. Gibt der Benutzer eine ungültige oder nicht vertrauenswürdige Domäne an, schlägt die Authentifizierung fehl.

Zwei Variablen, <NTUser> und <NTDomain>, ermöglichen Ihnen die individuelle Bezugnahme auf Domänen- und NT-Benutzernamenwerte. Das IVE gibt in diese beiden Variablen die Domäne und den NT-Benutzernamen ein.

HINWEIS: Wenn Sie vorhandene Rollenzuordnungsreglen verwenden oder eine neue Rollenzuordnungsregel für die Active Directory-Authentifizierung mittels USER = beliebigerbenutzername schreiben, behandelt das IVE diese Regel semantisch als NTUser = beliebigerbenutzername AND NTDomain = standarddomaene. Dadurch kann das IVE vorhandene Rollenzuordnungsregeln nahtlos einsetzen.

Unterstützung der Gruppensuche für Active Directory und NT

Das IVE unterstützt die Benutzergruppensuche in lokalen und globalen Gruppen der Domäne sowie in universellen Gruppen in der Active Directory-Gesamtstruktur als auch in lokalen und globalen Gruppen in der Domäne für NT4-Server.

Active Directory-Suche – Anforderungen

Das IVE unterstützt die Benutzergruppensuche in lokalen, globalen und universellen Gruppen in der Standarddomäne sowie in untergeordneten und in allen vertrauenswürdigen Domänen. Das IVE erhält die Gruppenmitgliedschaft über eine von drei Methoden, die unterschiedliche Merkmale aufweisen:

- **Gruppeninformationen im Sicherheitskontext des Benutzers** – Gibt Informationen über die globalen Gruppen in der Domäne des Benutzers zurück.
- **Gruppeninformationen durch LDAP-Suchaufrufe** – Gibt Informationen über die globalen Gruppen in der Domäne und die universellen Gruppen des Benutzers zurück, wenn das IVE den globalen Katalogserver abfragt.

- **Gruppeninformationen durch native RPC-Aufrufe** – Gibt Informationen über die lokale Gruppe in der Domäne des Benutzers zurück.

Hinsichtlich der Rollenzuordnungsregeln versucht das IVE die Gruppensuche in der folgenden Reihenfolge:

- Das IVE sucht unter Verwendung des Sicherheitskontexts des Benutzers nach allen globalen Gruppen in der Domäne.
- Das IVE stellt über eine LDAP-Abfrage den Status der Gruppenmitgliedschaft des Benutzers fest, wenn der Benutzer nicht Mitglied in den Gruppen ist, auf die sich die Rollenzuordnungsregeln beziehen.
- Das IVE ermittelt die Benutzerinformationen über RPC-Suchaufrufe, wenn der Benutzer nicht Mitglied einer lokalen Gruppe in der Domäne ist.

NT4-Gruppensuche – Anforderungen

Das IVE unterstützt die Gruppensuche in lokalen und globalen Gruppen, die in der Standarddomäne erstellt wurden, sowie in allen untergeordneten und in anderen vertrauenswürdigen Domänen. Das IVE ermittelt die Informationen der globalen Gruppe über den Sicherheitskontext des Benutzers und die lokalen Domäneninformationen über RPC-Aufrufe. In der NT4-Umgebung verwendet das IVE keine LDAP-basierten Suchaufrufe.

Definieren einer Active Directory-oder Windows NT-Domänenserverinstanz

So legen Sie einen Active Directory-Server oder einen Windows NT-Domänenserver fest:

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **Active Directory/ Windows NT** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des primären Domänencontrollers oder von Active Directory an.
5. Geben Sie die IP-Adresse des Sicherungsdomänencontrollers oder von Active Directory an. (Dies ist optional.)
6. Geben Sie den Domänennamen für die Benutzer ein, denen Sie den Zugriff gewähren möchten. Aktivieren Sie das Kontrollkästchen **Allow domain to be specified as part of username**, um es Benutzern zu ermöglichen, auf der IVE-Anmeldeseite im Feld **Username** einen Domänennamen im folgenden Format einzugeben: domaene\benutzername.

7. Geben Sie einen Administratorbenutzernamen und ein Kennwort für den Server ein. Für die AD/NT-Authentifizierung muss der angegebene Administrator ein Domänenadministrator sein.

HINWEIS: Nach dem Speichern von Änderungen wird das Kennwort unabhängig von der Kennwortlänge vom IVE mit fünf Sternchen maskiert.

8. Legen Sie unter **Authentication Protocol** das Protokoll fest, das das IVE während der Authentifizierung verwenden soll.

9. Führen Sie unter **Kerberos Realm Name** die folgenden Schritte aus:

   - Wenn das IVE den Kerberos-Bereichsnamen anhand der angegebenen Administrator-Anmeldeinformationen vom Active Directory-Server abrufen soll, wählen Sie **Use LDAP to get Kerberos realm name**.

   - Wenn Ihnen der Bereichsname bekannt ist, geben Sie den Kerberos-Bereichsnamen im Feld **Specify Kerberos realm name** ein.

10. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.

11. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll. Weitere Informationen finden Sie unter „Erstellen eines Authentifizierungsbereichs“ auf Seite 257.

HINWEIS: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 254.

Konfigurieren einer Instanz eines anonymen Servers

Die folgenden Themen werden behandelt:

- „Anonymer Server – Übersicht“ auf Seite 250
- „Definieren einer Instanz eines anonymen Servers“ auf Seite 251

Anonymer Server – Übersicht

Ein anonymer Server ermöglicht Benutzern den Zugriff auf das IVE ohne Angabe von Benutzername oder Kennwort. Wenn ein Benutzer den URL einer Anmeldeseite eingibt, für die die Authentifizierung durch einen anonymen Server konfiguriert ist, umgeht das IVE die IVE-Standardanmeldeseite und zeigt dem Benutzer sofort die IVE-Willkommensseite an.

Sie können anonyme Authentifizierung auswählen, wenn Sie es nicht für notwendig halten, dass die Ressourcen auf dem IVE sehr hohen Sicherheitsanforderungen unterliegen oder wenn Sie die anderen Sicherheitsmaßnahmen auf dem IVE für ausreichend halten. Sie können z. B. eine Benutzerrolle mit beschränktem Zugriff auf interne Ressourcen erstellen und diese Rolle dann mithilfe einer Richtlinie authentifizieren, die nur verlangt, dass sich Benutzer von einer IP-Adresse aus Ihrem internen Netzwerk anmelden. Bei dieser Methode wird davon ausgegangen, dass ein Benutzer, der zum Zugriff auf das interne Netzwerk berechtigt ist, auch die Ressourcen anzeigen darf, die im Rahmen dieser Benutzerrolle bereitgestellt werden.

Beachten Sie bei der Definition und Überwachung einer Instanz eines anonymen Servers Folgendes:

- Sie können nur eine Konfiguration für anonyme Server hinzufügen.
- Administratoren können nicht mithilfe eines anonymen Servers authentifiziert werden.
- Bei der Konfiguration müssen Sie auf der Registerkarte **Users > Authentication > General** den anonymen Server als Authentifizierungsserver und als Verzeichnis-/Attributserver auswählen. Weitere Informationen finden Sie unter „Registerkarte „General““ auf Seite 257.
- Beim Erstellen von Rollenzuordnungsregeln auf der Registerkarte **Users > Authentication > Role Mapping** (siehe „Registerkarte „Role Mapping““ auf Seite 260) lässt das IVE die Erstellung von Zuordnungsregeln für bestimmte Benutzer (z. B. „Joe“) nicht zu, da auf dem anonymen Server keine Informationen zu Benutzernamen gespeichert werden. Sie können Rollenzuordnungsregeln erstellen, die auf einem Standardbenutzernamen (*) oder Zertifikatattributen basieren.
- Aus Sicherheitsgründen können Sie ggf. die Anzahl der Benutzer beschränken, die sich gleichzeitig über einen anonymen Server anmelden. Verwenden Sie dazu die Option auf der Registerkarte **Users > Authentication > [Bereich] > Authentication Policy > Limits**. Dabei ist **[Bereich]** der Bereich, der für die Benutzerauthentifizierung durch den anonymen Server konfiguriert ist. Weitere Informationen finden Sie unter „Begrenzungen für gleichzeitig angemeldete Benutzer“ auf Seite 260.

- Sie können die Sitzungen von anonymen Benutzern (im Gegensatz zu anderen Authentifizierungsservern) nicht löschen und nicht über die Registerkarte **Users** anzeigen, da keine Benutzernamen eingegeben wurden und das IVE daher keine individuellen Sitzungsdaten anzeigen kann.

Definieren einer Instanz eines anonymen Servers

So definieren Sie einen anonymen Server:

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **Anonymous Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Klicken Sie auf **Save Changes**.
5. Geben Sie die Bereiche an, die der Server für die Autorisierung von Benutzern verwenden soll. Weitere Informationen finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich“ auf Seite 260.

Konfigurieren einer Zertifikatserverinstanz

Die folgenden Themen werden behandelt:

- „Zertifikatserver – Übersicht“ auf Seite 252
- „Festlegen einer Zertifikatserverkonfiguration“ auf Seite 252

Zertifikatserver – Übersicht

Der Zertifikatserver ermöglicht die Authentifizierung von Benutzern anhand von Attributen in clientseitigen Zertifikaten. Sie können den Zertifikatserver allein oder in Verbindung mit einem anderen Server verwenden, um Benutzer zu authentifizieren und sie Rollen zuzuordnen.

Sie könnten Benutzer z. B. allein anhand ihrer Zertifikatattribute authentifizieren. Wenn das IVE ermittelt, dass das Benutzerzertifikat gültig ist, wird der Benutzer anhand der von Ihnen festgelegten Zertifikatattribute angemeldet, ohne aufgefordert zu werden, einen Benutzernamen oder ein Kennwort einzugeben.

Sie können Benutzer auch authentifizieren, indem Sie ihre Clientzertifikatattribute an einen zweiten Authentifizierungsserver (wie LDAP) weiterleiten. In diesem Szenario ermittelt der Zertifikatserver zunächst, ob das Benutzerzertifikat gültig ist. Anschließend kann das IVE Zuordnungsregeln der Bereichsebene verwenden, um die Zertifikatattribute mit den LDAP-Attributen des Benutzers zu vergleichen. Wenn keine entsprechende Übereinstimmung gefunden wird, kann der Benutzerzugriff entsprechend Ihren Angaben vom IVE verweigert oder eingeschränkt werden.

HINWEIS: Bei Verwendung clientseitiger Zertifikate ist dringend zu empfehlen, die Endbenutzer anzuweisen, ihre Webbrowser nach dem Abmelden vom IVE zu schließen. Andernfalls können andere Benutzer über deren geöffnete Browsersitzungen auf durch Zertifikate geschützte Ressourcen auf dem IVE ohne erneute Authentifizierung zugreifen. (Nach dem Laden eines clientseitigen Zertifikats werden die Anmeldedaten und der private Schlüssel des Zertifikats von Internet Explorer zwischengespeichert. Diese Informationen bleiben in den Browsern zwischengespeichert, bis der Browser vom Benutzer geschlossen wird (in manchen Fällen, bis die Arbeitsstation neu gestartet wird). Ausführliche Informationen finden Sie unter: http://support.microsoft.com/?kbid=290345.) Sie können die Benutzer daran erinnern, ihren Browser zu schließen, indem Sie die Meldung für die Abmeldung auf der Registerkarte **System > Signing In > Sign-in Pages** ändern.

Festlegen einer Zertifikatserverkonfiguration

Gehen Sie zum Festlegen eines Zertifikatservers auf dem IVE folgendermaßen vor:

1. Verwenden Sie die Einstellungen auf der Registerkarte **System > Configuration > Certificates > CA Certificates**, um das zum Signieren der clientseitigen Zertifikate verwendete Zertifikat der Zertifizierungsstelle zu importieren.
2. Konfigurieren Sie eine Zertifikatserverinstanz:
   a. Wählen Sie **Signing In > AAA Servers**.

b. Wählen Sie in der Liste **New** die Option **Certificate Server**, und klicken Sie dann auf **New Server**.

c. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.

d. Geben Sie im Feld **User Name Template** an, wie das IVE einen Benutzernamen erstellen soll. Sie können jede beliebige Kombination von Zertifikatsvariablen in spitzen Klammern und Klartext verwenden.

e. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.

HINWEIS: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 254.

3. Wenn Zertifikatattribute mithilfe eines LDAP-Servers überprüft werden sollen, erstellen Sie anhand der Einstellungen auf der Seite **Signing In > AAA Servers** eine LDAP-Serverinstanz. Beachten Sie, dass Sie zum Abrufen der benutzerspezifischen Attribute, die über das Zertifikat überprüft werden sollen, den Abschnitt **Finding user entries** auf der LDAP-Konfigurationsseite verwenden müssen.

4. Legen Sie anhand der Einstellungen auf den Registerkarten **Users > Authentication > Authentication > General** bzw. **Administrators > Authentication > General** fest, welche Bereiche den Zertifikatserver zum Authentifizieren von Benutzern verwenden sollen. (Anhand der Einstellungen dieser Registerkarten können Sie auch Bereiche angeben, die einen LDAP-Server zum Überprüfen von Zertifikatattributen verwenden sollen.)

5. Ordnen Sie anhand der Einstellungen auf der Seite **Signing In > Sign-in > Sign-in Policies** die im vorherigen Schritt konfigurierten Bereiche einzelnen Anmelde-URLs zu.

6. Wenn der Benutzerzugriff auf Bereiche, Rollen oder Ressourcenrichtlinien auf Grundlage einzelner Zertifikatattribute eingeschränkt werden soll, verwenden Sie die unter „Zertifikateinschränkungen“ auf Seite 421 beschriebenen Einstellungen.

Anzeigen und Löschen von Benutzersitzungen

Die Konfigurationsseite für die meisten IVE-Authentifizierungsserver enthält eine Registerkarte **Users**, auf der Sie aktive IVE-Benutzersitzungen anzeigen und löschen können. Auf den folgenden Typen von Authentifizierungsservern wird diese Registerkarte nicht angezeigt:

- **Anonymer Server** – Das IVE kann keine individuellen Sitzungsdaten für Benutzer anzeigen, die sich über einen anonymen Server anmelden, da bei der Benutzeranmeldung über einen anonymen Server keine Benutzernamen oder anderen Anmeldeinformationen erfasst werden.

- **Lokaler Authentifizierungsserver** – Das IVE zeigt für lokale Authentifizierungsserver anstelle einer Registerkarte **Users** eine Registerkarte **Local Users** an, auf der Sie Benutzerkonten hinzufügen und löschen können (anstelle von Benutzersitzungen).

Bei sämtlichen anderen Typen von Authentifizierungsservern können Sie aktive Benutzersitzungen anzeigen und löschen. Folgen Sie hierfür den folgenden Anweisungen.

So zeigen Sie eine aktive Benutzersitzung an oder löschen sie:

1. Wählen Sie in der Webkonsole **Signing In > AAA Servers** aus.
2. Klicken Sie in der Liste **Authentication/Authorization Servers** auf die entsprechende Verknüpfung.
3. Klicken Sie auf die Registerkarte **Users**.
4. Führen Sie eine der folgenden Aufgaben durch:
   - Geben Sie im Feld **Show users named** einen Benutzernamen ein, und klicken Sie auf **Update**, um nach einem bestimmten Benutzer zu suchen.

     Sie können auch ein Sternchen (*) als Platzhalter verwenden, das für eine beliebige Anzahl von Zeichen steht (null, eins oder mehrere). Wenn Sie z. B. nach allen Benutzernamen suchen möchten, die die Buchstaben jo enthalten, geben Sie im Feld **Show users named** die Zeichenfolge *jo* ein. Bei der Suche wird die Groß- und Kleinschreibung berücksichtigt. Wenn Sie wieder die gesamte Liste der Gruppenkonten anzeigen möchten, geben Sie ein Sternchen (*) ein, oder löschen Sie den Feldinhalt, und klicken Sie dann auf **Update**.

   - Geben Sie im Feld **Show N users** eine Zahl ein, und klicken Sie auf **Update**, um die Anzahl von Benutzern anzugeben, die auf der Seite angezeigt werden.

   - Aktivieren Sie das Kontrollkästchen neben den jeweiligen Benutzern, und klicken Sie anschließend auf **Delete**, um deren IVE-Sitzungen zu beenden.

Kapitel 8

Administratoreinstellungen

Auf der Webkonsole können Sie mithilfe der Einstellungen im Abschnitt **Administrators** Administratorauthentifizierungsbereiche und delegierte Administratorrollen erstellen und konfigurieren.

Inhalt

- „Konfigurieren der Seite „Authentication““ auf Seite 257
- „Konfigurieren der Seite „Delegation““ auf Seite 267

Konfigurieren der Seite „Authentication“

Über die Menüs **Administrators > Authentication** und **Users > Authentication** können Benutzer auf die entsprechenden Seiten für **Authentication Realms** zugreifen. Auf diesen Seiten können Sie Authentifizierungsbereiche im System erstellen und verwalten.

Die Seite **Authentication Realms** enthält die folgenden Registerkarten:

- „Registerkarte „General““ auf Seite 257 – Verwenden Sie diese Registerkarte, um einen Authentifizierungsbereich zu erstellen.
- „Registerkarte „Authentication Policy““ auf Seite 259 – Verwenden Sie diese Registerkarte, um eine Richtlinie für einen Authentifizierungsbereich anzugeben.
- „Registerkarte „Role Mapping““ auf Seite 260 – Verwenden Sie diese Registerkarte, um Rollenzuordnungsregeln festzulegen und den Serverkatalog zu verwenden.

Registerkarte „General“

Auf der Registerkarte **General** können Sie einen Authentifizierungsbereich erstellen. Weitere Informationen zu Bereichen finden Sie unter „Authentifizierungsbereiche – Übersicht“ auf Seite 51.

Erstellen eines Authentifizierungsbereichs

So erstellen Sie einen Authentifizierungsbereich:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Authentication** oder **Users > Authentication** aus.
2. Klicken Sie auf der entsprechenden Seite **Authentication Realms** auf **New**.
3. Gehen Sie auf der Seite **New Authentication Realm** folgendermaßen vor:
   a. Geben Sie eine Bezeichnung für diesen Bereich ein.
   b. Geben Sie eine Beschreibung für den Bereich ein. (Dies ist optional.)
   c. Aktivieren Sie **When editing, start on the Role Mapping page**, wenn die Registerkarte **Role Mapping** beim Öffnen des Bereichs zur Bearbeitung aktiviert sein soll.
4. Legen Sie unter **Servers** Folgendes fest:
   - Einen Authentifizierungsserver, der zum Authentifizieren von Benutzern verwendet werden soll, die sich bei diesem Bereich anmelden.
   - Einen Verzeichnis-/Attributserver zum Abrufen von Benutzerattributen und Gruppeninformationen für Rollenzuordnungsregeln und Ressourcenrichtlinien. (Dies ist optional.)

- Einen RADIUS-Server, der festhält, wann sich ein Benutzer im IVE anmeldet und sich daraus wieder abmeldet (optional).

5. Geben Sie unter **Additional authentication server** an, ob Sie die zweistufige Authentifizierung für den Zugriff auf das IVE aktivieren möchten. So aktivieren Sie einen zweiten Authentifizierungsserver:

   a. Wählen Sie den Namen des zweiten Authentifizierungsservers. Sie können keinen anonymen Server oder Zertifikatserver verwenden.

   b. Aktivieren Sie **Username is specified by user on sign-in page**, wenn der Benutzer während der Anmeldung am IVE aufgefordert werden soll, am zweiten Server seinen Benutzernamen manuell einzugeben. Wenn andernfalls automatisch ein Benutzername an den zweiten Server übermittelt werden soll, geben Sie ins Feld **predefined as** statischen Text oder eine Variable ein. Das IVE übermittelt standardmäßig die Sitzungsvariable <username>, die denselben Benutzernamen enthält, der auch zur Anmeldung am primären Authentifizierungsserver verwendet wird.

   c. Aktivieren Sie **Password is specified by user on sign-in page**, wenn der Benutzer während der Anmeldung am IVE aufgefordert werden soll, am zweiten Server sein Kennwort manuell einzugeben. Wenn andernfalls automatisch ein Kennwort an den zweiten Server übermittelt werden soll, geben Sie ins Feld **predefined as** (Vordefiniert als) statischen Text oder eine Variable ein.

   d. Aktivieren Sie **End session if authentication against this server fails**, wenn der Zugriff auf das IVE von der erfolgreichen Anmeldung des Benutzers am zweiten Server abhängen soll.

6. Wählen Sie unter **Dynamic policy evaluation** Optionen aus, wenn Sie dynamische Richtlinienauswertung für diesen Bereich verwenden möchten (siehe „Dynamic Policy Evaluation (Dynamische Richtlinienauswertung)“ auf Seite 44):

   a. Wählen Sie **Enable dynamic policy evaluation**, um einen automatischen Timer für die dynamische Richtlinienauswertung der Authentifizierungsrichtlinie, Rollenzuordnungsregeln und Rolleneinschränkungen dieses Bereichs zu aktivieren. Nach dem Aktivieren dieser Option, verwenden Sie die Option **Refresh interval**, um festzulegen, wie oft das IVE eine automatische Richtlinienauswertung aller aktuell angemeldeten Bereichsbenutzer durchführen soll. Sie müssen die Option **Enable dynamic policy evaluation** aktivieren, damit die Einstellungen für **Refresh interval**, **Refresh roles** und **Refresh resource policies** wirksam werden.

   b. Bei **Refresh interval** geben Sie die Anzahl der Minuten an (5 bis 1440), die das IVE warten soll, bevor jede automatische, zeitabhängige Richtlinienauswertung durchgeführt werden soll.

   c. Wählen Sie **Refresh roles**, um die Option **Enable dynamic policy evaluation** so zu erweitern, dass die Rollen aller Benutzer in diesem Bereich ebenfalls aktualisiert werden. (Diese Option wirkt sich nicht auf die Funktion der Schaltfläche **Refresh Now** aus.)

d. Wählen Sie **Refresh resource policies** , um die Option **Enable dynamic policy evaluation** so zu erweitern, dass die Ressourcenrichtlinien (Meeting und Email Client nicht eingeschlossen) aller Benutzer in diesem Bereich ebenfalls aktualisiert werden. (Diese Option wirkt sich nicht auf die Funktion der Schaltfläche **Refresh Now** aus.)

HINWEIS: Wenn Sie **Enable dynamic policy evaluation** wählen und **Refresh roles** und **Refresh resource policies** nicht aktivieren, wertet das IVE *nur* die Authentifizierungsrichtlinie, die Rollenzuordnungsregeln und Rolleneinschränkungen des Bereichs aus.

---

e. Klicken Sie auf **Refresh Now**, um die Authentifizierungsrichtlinie, die Rollenzuordnungsregeln, Rolleneinschränkungen, Benutzerrollen und Ressourcenrichtlinien des Bereichs für alle aktuell angemeldeten Bereichsbenutzer manuell auszuwerten. Verwenden Sie diese Schaltfläche, wenn Sie Änderungen an einer Authentifizierungsrichtlinie, an Rollenzuordnungsregeln, Rolleneinschränkungen oder Ressourcenrichtlinien vornehmen möchten, und die Rollen der Benutzer dieses Bereichs sofort aktualisiert werden sollen.

HINWEIS: Da die dynamische Richtlinienauswertung die Systemleistung möglicherweise beeinträchtigt, beachten Sie folgende Richtlinien:

- Weil das automatische (timerbasierte) Aktualisieren von Benutzerrollen und Ressourcenrichtlinien die Systemleistung beeinträchtigen kann, haben Sie die Möglichkeit, die Leistung zu verbessern, indem Sie eine der Optionen oder die beiden Optionen **Refresh roles** und **Refresh resource policies** deaktivieren; so werden die Auswirkungen der Aktualisierung gemindert.
- Zur Verbesserung der Leistung setzen Sie die Option **Refresh interval** auf ein längeres Zeitintervall.
- Verwenden Sie die Schaltfläche **Refresh Now**, wenn die Benutzer davon nicht betroffen sein sollen.

---

7. Klicken Sie auf **Save Changes**, um den Bereich auf dem IVE zu erstellen. Die Registerkarten **General**, **Authentication Policy** und **Role Mapping** für den Authentifizierungsbereich werden angezeigt.
8. Führen Sie die nächsten Konfigurationsschritte aus:
   a. Konfigurieren Sie mindestens eine Rollenzuordnungsregel wie unter „Registerkarte „Role Mapping““ auf Seite 260 beschrieben.
   b. Konfigurieren Sie eine Authentifizierungsrichtlinie für den Bereich wie unter „Registerkarte „Authentication Policy““ auf Seite 259 beschrieben.

Registerkarte „Authentication Policy“

Auf der Registerkarte **Authentication Policy** können Sie eine Richtlinie für einen Authentifizierungsbereich erstellen. Weitere Informationen zu Bereichen finden Sie unter „Authentifizierungsbereiche – Übersicht“ auf Seite 51.

Angeben einer Richtlinie für einen Authentifizierungsbereich

So geben Sie eine Richtlinie für einen Authentifizierungsbereich an:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Authentication** oder **Users > Authentication** aus.
2. Wählen Sie auf der entsprechenden Seite **Authentication Realms** einen Bereich aus, und klicken Sie dann auf die Registerkarte **Authentication Policy**.
3. Konfigurieren Sie auf der Seite **Authentication Policy** mindestens eine der in den folgenden Abschnitten beschriebenen Zugriffsverwaltungsoptionen:
   - „Angeben von IP-Quelladresseinschränkungen“ auf Seite 418
   - „Angeben von Browsereinschränkungen“ auf Seite 419
   - „Angeben clientseitiger Zertifikateinschränkungen“ auf Seite 421
   - „Angeben einer Kennwortlängeneinschränkung“ auf Seite 422
   - „Angeben von Host Checker-Einschränkungen“ auf Seite 423
   - „Angeben von Cache Cleaner-Einschränkungen“ auf Seite 425[1]
   - „Begrenzungen für gleichzeitig angemeldete Benutzer“ auf Seite 260

Begrenzungen für gleichzeitig angemeldete Benutzer

Neben den Zugriffsverwaltungsoptionen, die Sie für eine Authentifizierungsrichtlinie festlegen können, können Sie auch die Höchstanzahl gleichzeitig angemeldeter Benutzer festlegen. Konfigurieren Sie diese Einstellung hier:

- Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Limits
- Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Limits

Nur wenn ein Benutzer, der auf einer der Anmeldeseiten dieses Bereichs einen URL eingibt, alle für die Authentifizierungsrichtlinie festgelegten Benutzeranforderungen hinsichtlich Zugriffsverwaltung und gleichzeitig angemeldeter Benutzer erfüllt, öffnet das IVE die Anmeldeseite.

Registerkarte „Role Mapping“

Auf der Registerkarte **Role Mapping** können Sie Rollenzuordnungsregeln für einen Authentifizierungsbereich festlegen. Entsprechende Informationen finden Sie auf folgenden Seiten:

- Bereiche siehe „Authentifizierungsbereiche – Übersicht“ auf Seite 51.
- Rollen siehe „Benutzerrollen – Übersicht“ auf Seite 56.

1. In Administratorbereichen nicht verfügbar.

Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich

Zum Erstellen einer neuen Regel, die LDAP-Benutzerattribute oder -Gruppeninformationen verwendet, müssen Sie den Serverkatalog verwenden. Informationen zu diesem Katalog finden Sie unter „Verwenden des LDAP-Serverkatalogs“ auf Seite 263.

So geben Sie Rollenzuordnungsregeln für einen Authentifizierungsbereich an:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Authentication** oder **Users > Authentication** aus.

2. Wählen Sie auf der entsprechenden Seite **Authentication Realms** einen Bereich aus, und klicken Sie dann auf die Registerkarte **Role Mapping**.

3. Klicken Sie auf **New Rule**, um auf die Seite **Role Mapping Rule** zuzugreifen. Diese Seite stellt einen integrierten Editor für die Definition von Regeln bereit.

4. Wählen Sie in der Liste **Rule based on** eines der folgenden Elemente aus:

   - **Username** – *Username* ist der IVE-Benutzername, der auf der Anmeldeseite eingegeben wird. Wählen Sie diese Option aus, wenn Benutzer anhand ihrer IVE-Benutzernamen zu Rollen zugeordnet werden sollen. Dieser Regeltyp ist für alle Bereiche verfügbar.

   - **User attribute** – *User attribute* ist ein Benutzerattribut von einem RADIUS- oder LDAP-Server. Wählen Sie diese Option aus, wenn Benutzer anhand eines Attributs vom entsprechenden Server Rollen zugeordnet werden sollen. Dieser Regeltyp steht nur für Bereiche zur Verfügung, die einen RADIUS-Server als Authentifizierungsserver oder einen LDAP-Server als Authentifizierungs- bzw. Verzeichnisserver verwenden. Nachdem Sie die Option **User attribute** gewählt haben, klicken Sie auf **Update**, um die Liste **Attribute** und die Schaltfläche **Attributes** anzuzeigen. Zum Anzeigen des Serverkatalogs klicken Sie auf die Schaltfläche **Attributes**. Informationen zum Hinzufügen von LDAP-Benutzerattributen unter Verwendung des Serverkatalogs finden Sie unter „Verwenden des LDAP-Serverkatalogs“ auf Seite 263).

   - **Certificate or Certificate attribute** – *Certificate* oder *Certificate attribute* ist ein Attribut, das vom clientseitigen Zertifikat des Benutzers unterstützt wird. Wählen Sie diese Option, wenn Benutzer anhand ihrer Zertifikatsattribute Rollen zugeordnet werden sollen. Die Option *Certificate* ist für alle Bereiche verfügbar, während die Option *Certificate attribute* nur für Bereiche verfügbar ist, die einen LDAP-Authentifizierungs- oder Verzeichnisserver verwenden. Nach dem Auswählen dieser Option klicken Sie auf **Update**, um das Textfeld **Attribute** anzuzeigen.

- **Group membership** – *Group membership* ist eine Angabe zur Gruppe von einem LDAP-Server oder systemeigenen Active Directory-Server, die Sie der Registerkarte **Groups** des Serverkatalogs hinzufügen. Wählen Sie diese Option aus, wenn Benutzer anhand der LDAP- bzw. Active Directory-Gruppeninformationen Rollen zugeordnet werden sollen. Dieser Regeltyp steht nur für Bereiche zur Verfügung, die einen LDAP-Server als Authentifizierungs- oder Verzeichnisserver verwenden oder die einen Active Directory-Server für die Authentifizierung verwenden. (Ein Active Directory-Server kann nicht als Autorisierungsserver für einen Bereich angegeben werden.)

5. Geben Sie unter **Rule** die auszuwertende Bedingung an, die dem ausgewählten Regeltyp entspricht und folgende Punkte umfasst:

   a. Angeben von mindestens einem Benutzernamen, RADIUS- oder LDAP-Benutzerattribut, Zertifikatsattribut oder einer LDAP-Gruppe.

   b. Angeben der Wertentsprechungen. Dies kann auch eine Liste von IVE-Benutzernamen, Benutzerattributswerten von einem RADIUS- oder LDAP-Server, clientseitigen Zertifikatswerten (statische oder LDAP-Attributwerte) oder LDAP-Gruppen umfassen.

6. Nehmen Sie unter **...then assign these roles** folgende Eingaben vor:

   a. Geben Sie die Rollen an, die Sie dem authentifizierten Benutzer zuordnen möchten, indem Sie Rollen zur Liste **Selected Roles** hinzufügen.

   b. Aktivieren Sie die Option **Stop processing rules when this rule matches**, wenn das IVE die Auswertung der Rollenzuordnungsregeln anhalten soll, wenn der Benutzer die für diese Regel angegebenen Bedingungen erfüllt.

7. Klicken Sie auf **Save Changes**, um die Regel auf der Registerkarte **Role Mapping** zu erstellen. Gehen Sie nach dem Abschluss der Regelerstellung folgendermaßen vor:

   - Bringen Sie die Regeln unbedingt in die Reihenfolge, in der das IVE diese auswerten soll. Diese ist besonders dann wichtig, wenn die Verarbeitung der Rollenzuordnungsregeln bei einer Übereinstimmung angehalten werden soll.

   - Geben Sie an, ob die Einstellungen für alle zugeordneten Rollen zusammengeführt werden sollen. Siehe „Richtlinien für permissive Zusammenführungen“ auf Seite 58.

Verwenden des LDAP-Serverkatalogs

Der *LDAP-Server Catalog* ist ein sekundäres Fenster, in dem Sie LDAP-Zusatzinformationen angeben können, die das IVE für die Zuordnung von Benutzern zu Rollen verwendet, darunter:

- **Attributes** – Auf der Registerkarte **Server Catalog Attributes** wird eine Liste allgemeiner LDAP-Attribute angezeigt, z. B. cn, uid, uniquemember und memberof. Diese Registerkarte kann nur beim Zugriff auf den Serverkatalog eines LDAP-Servers aufgerufen werden. Auf dieser Registerkarte können Sie die Attribute eines LDAP-Servers verwalten, indem Sie seinem IVE-Serverkatalog benutzerdefinierte Werte hinzufügen oder Werte aus diesem löschen. Beachten Sie, dass das IVE eine lokale Kopie der LDAP-Serverwerte aufbewahrt. Attribute werden dem Wörterbuch weder hinzugefügt noch aus diesem gelöscht.

- **Groups** – Über die Registerkarte **Server Catalog Groups** können Gruppeninformationen einfach von einem LDAP-Server abgefragt und dem Serverkatalog eines IVE-Servers hinzugefügt werden. Sie geben den BaseDN der Gruppen und ggf. einen Filter an, um die Suche zu starten. Wenn Ihnen der genaue Container der Gruppen nicht bekannt ist, können Sie den Domänenstamm als BaseDN festlegen, z. B. dc=juniper, dc=com. Die Suchseite gibt eine Gruppenliste vom Server zurück, aus der Sie Gruppen auswählen können, die in die Liste **Groups** eingegeben werden.

HINWEIS: Der auf der Konfigurationsseite des LDAP-Servers unter „Finding user entries“ angegebene BaseDN-Wert ist der Standard-BaseDN-Wert. Der Filterwert ist standardmäßig auf (cn = *) gesetzt.

Sie können Gruppen auch auf der Registerkarte **Groups** angeben. Sie müssen den FQDN (Fully Qualified Distinguished Name) einer Gruppe angeben, z. B. cn = Manager, ou = Zentrale, ou = Juniper, o = com, c = DE, können dieser Gruppe jedoch eine Bezeichnung zuordnen, die in der Liste **Groups** angezeigt wird. Beachten Sie, dass diese Registerkarte nur beim Zugriff auf den Serverkatalog eines LDAP-Servers aufgerufen werden kann.

Anzeigen des LDAP-Serverkatalogs:

1. Nachdem Sie auf der Seite **Role Mapping Rule** (siehe „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 261) die Option **User attribute** ausgewählt haben, klicken Sie auf **Update**, um die Liste **Attribute** und die Schaltfläche **Attributes** anzuzeigen.

2. Zum Anzeigen des LDAP-Serverkatalogs klicken Sie auf die Schaltfläche **Attributes**.

Abbildung 31: Registerkarte „Server Catalog > Attributes“ – Hinzufügen eines Attributs für LDAP

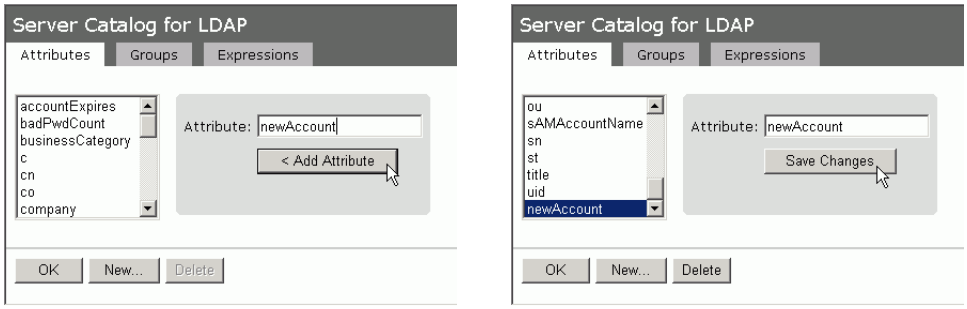


Abbildung 32: Das im Serverkatalog hinzugefügte Attribut steht für die Rollenzuordnungsregel zur Verfügung.

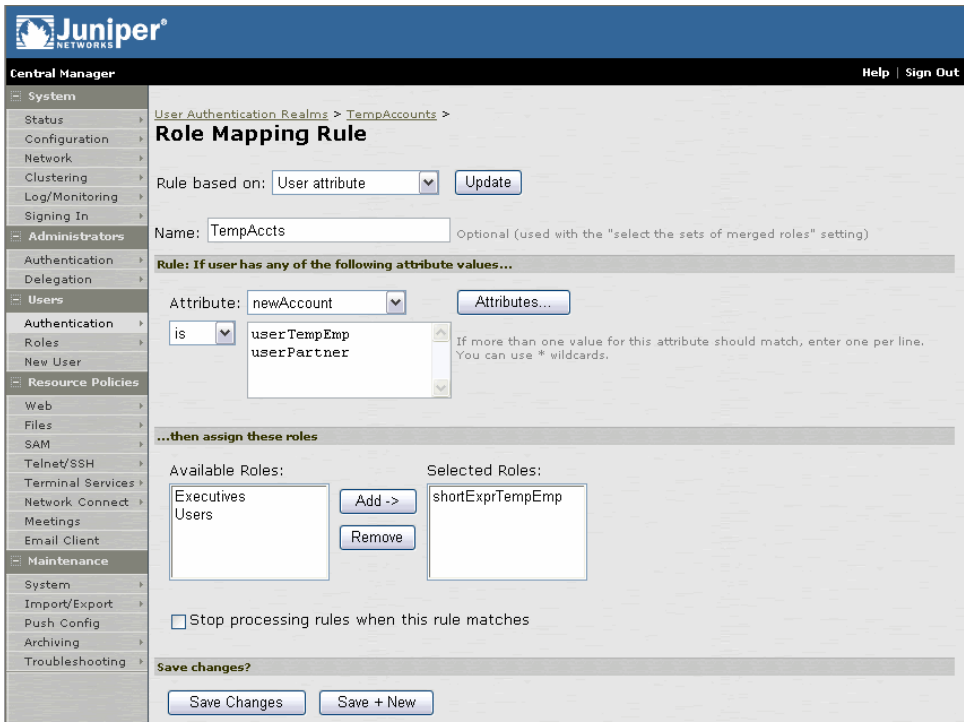


Abbildung 33: Registerkarte „Server Catalog > Groups“ – Hinzufügen von LDAP-Gruppen

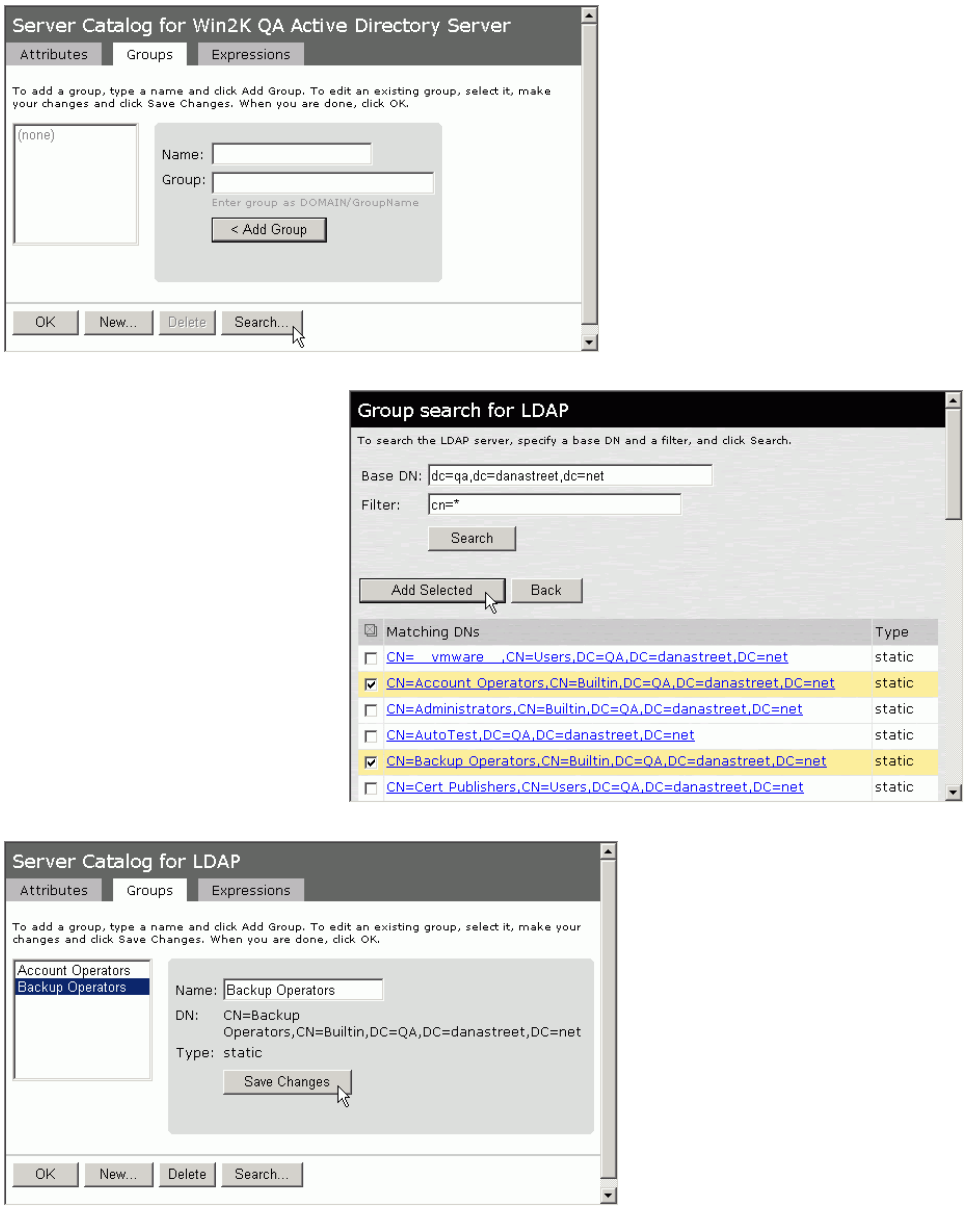
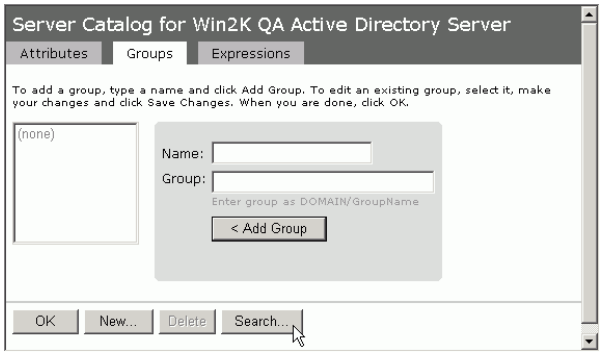
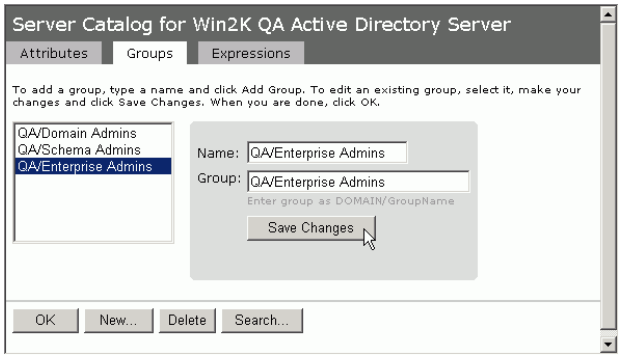


Abbildung 34: Registerkarte „Server Catalog > Groups“ – Hinzufügen von Active Directory-Gruppen


Server Catalog for Win2K QA Active Directory Server
Attributes
Groups
Expressions
To add a group, type a name and click Add Group. To edit an existing group, select it, make your changes and click Save Changes. When you are done, click OK.
(none)
Name:
Group:
Enter group as DOMAIN/GroupName
< Add Group
OK
New...
Delete
Search...


Server Catalog for Win2K QA Active Directory Server
Attributes
Groups
Expressions
To add a group, type a name and click Add Group. To edit an existing group, select it, make your changes and click Save Changes. When you are done, click OK.
QA/Domain Admins
QA/Schema Admins
QA/Enterprise Admins
Name: QA/Enterprise Admins
Group: QA/Enterprise Admins
Enter group as DOMAIN/GroupName
Save Changes
OK
New...
Delete
Search...

Konfigurieren der Seite „Delegation“

Eine *Administratorrolle* ist eine definierte Einheit, die IVE-Verwaltungsfunktionen und Sitzungseigenschaften für die der Rolle zugeordneten Administratoren angibt.

Die Seite **Delegation** enthält die folgenden Registerkarten:

- „Registerkarten „General““ auf Seite 267 – Auf diesen Registerkarten können Sie allgemeine Rolleneigenschaften, Zugriffsverwaltungsbeschränkungen, Sitzungsoptionen und Schnittstelleneinstellungen festlegen.

Konfigurieren von Administratorrollen

Wenn Sie zu **Administrators > Delegation** navigieren, wird die Seite **Delegated Admin Roles** angezeigt. Auf dieser Seite können Sie Standardbenutzeroptionen für Sitzungen und die Benutzeroberfläche für Administratorrollen festlegen.

Ändern von Administratorrollen

So ändern Sie eine vorhandene Administratorrolle:

1. Wählen Sie in der Webkonsole die Option **Administrators > Delegation** aus.
2. Klicken Sie auf den Namen der zu ändernden Administratorrolle.
3. Ändern Sie die Rolleneinstellungen nach den Anweisungen in: „Registerkarten „General““ auf Seite 267.

Registerkarten „General“

Mit den Unterregisterkarten **General** können Sie allgemeine Rolleneigenschaften, Zugriffsverwaltungsbeschränkungen, Sitzungsoptionen und Schnittstelleneinstellungen festlegen.

Registerkarte „Overview“

Verwalten allgemeiner Einstellungen und Optionen für Rollen

Auf der Registerkarte **General > Overview** können Sie den Namen und die Beschreibung einer Rolle bearbeiten sowie Sitzungs- und Benutzeroberflächenoptionen aktivieren und deaktivieren.

So verwalten Sie allgemeine Einstellungen und Optionen für Rollen:

1. Klicken Sie in der Webkonsole auf **Administrators > Delegation >** *Rollenname* **> General > Overview**.
2. Erstellen Sie anhand der Felder **Name** und **Description** (optional) eine Bezeichnung für die delegierte Administratorrolle.

3. Aktivieren Sie unter **Options** folgende Kontrollkästchen:

   - **Session Options**, um die auf der Registerkarte **General > Session Options** konfigurierten Einstellungen auf die Rolle anzuwenden.

   - **UI Options**, um die auf der Registerkarte **General > UI Options** konfigurierten Einstellungen auf die Rolle anzuwenden.

4. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

Registerkarte „Restrictions“

Legen Sie auf der Registerkarte **General > Restrictions** Zugriffsverwaltungsoptionen für die Rolle fest. Administratoren werden der Rolle vom IVE nur dann zugeordnet, wenn Sie die angegebenen Einschränkungen erfüllen. Weitere Informationen zur Zugriffsverwaltung finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 38.

Festlegen von Zugriffsverwaltungsoptionen für die Rolle

So legen Sie Zugriffsverwaltungsoptionen für die Rolle fest:

1. Klicken Sie in der Webkonsole auf **Administrators > Delegation >** *Rollenname* **> General > Restrictions**.

2. Klicken Sie auf die Registerkarte der Option, die Sie für die Rolle konfigurieren möchten, und konfigurieren Sie sie gemäß den Anweisungen in den folgenden Abschnitten:

   - „Angeben von IP-Quelladresseinschränkungen“ auf Seite 418

   - „Angeben von Browsereinschränkungen“ auf Seite 419

   - „Angeben clientseitiger Zertifikateinschränkungen“ auf Seite 421

   - „Angeben von Host Checker-Einschränkungen“ auf Seite 423

   Für die Rolle kann eine beliebige Anzahl von Zugriffsverwaltungsoptionen konfiguriert werden. Wenn ein Administrator nicht alle Einschränkungen erfüllt, dann ordnet das IVE den Administrator der Rolle nicht zu.

3. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

Registerkarte „Session Options“

Auf der Registerkarte **General > Session Options** können Sie Sitzungszeitbegrenzungen und Roamingfunktionen angeben. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **Session Options**, um diese Einstellungen für die Rolle zu aktivieren.

Angeben von Sitzungszeit- und Roamingeinstellungen für Benutzer

So geben Sie allgemeine Sitzungsoptionen an:

1. Klicken Sie in der Webkonsole auf **Administrators > Delegation >** *Rollenname* **> General > Session Options**.

2. Geben Sie unter **Session Lifetime** Werte für folgende Optionen an:

   - **Idle Timeout** – Geben Sie die Anzahl der Minuten an, die sich eine Administratorsitzung im Leerlauf befinden kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Das Inaktivitätszeitlimit für Sitzungen beträgt in der Standardeinstellung zehn Minuten, d. h., eine Administratorsitzung, die zehn Minuten lang inaktiv ist, wird vom IVE beendet, und das Ereignis wird im Systemprotokoll erfasst (sofern Sie nicht die unten beschriebenen Warnungen bei Sitzungszeitüberschreitung aktivieren).

   - **Max. Session Length** – Geben Sie die Anzahl der Minuten an, die eine aktive Administratorsitzung geöffnet bleiben kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Standardzeitbegrenzung für eine Administratorsitzung beträgt sechzig Minuten. Nach dieser Zeitspanne beendet das IVE die Sitzung und protokolliert das Ereignis im Systemprotokoll.

3. Geben Sie unter **Roaming session** Folgendes an:

   - **Enabled** – Ermöglicht Roamingbenutzersitzungen für Benutzer, die dieser Gruppe zugeordnet sind. Eine Roamingbenutzersitzung funktioniert über Quell-IP-Adressen, wodurch sich mobile Administratoren (Benutzer von Laptops) mit dynamischen IP-Adressen von einem Standort aus beim IVE anmelden und ihre Arbeit von einem anderen Standort fortsetzen können. Einige Browser weisen jedoch eventuell Schwachstellen auf, über die durch bösartigen Code Benutzercookies gestohlen werden können. Ein böswilliger Benutzer kann dann ein gestohlenes IVE-Sitzungscookie verwenden, um sich beim IVE anzumelden.

   - **Limit to subnet** – Beschränkt die Roamingsitzung auf das lokale Subnetz, das im Feld **Netmask** angegeben ist. Administratoren können sich von einer IP-Adresse aus anmelden und ihre Sitzungen mit einer anderen IP-Adresse fortsetzen, sofern sich die neue IP-Adresse in demselben Subnetz befindet.

   - **Disabled** – Deaktiviert Roamingsitzungen für Administratoren, die dieser Rolle zugeordnet sind. Administratoren, die sich von einer IP-Adresse aus anmelden, können eine aktive IVE-Sitzung nicht von einer anderen IP-Adresse aus fortsetzen. Administratorsitzungen sind an die ursprüngliche Quell-IP-Adresse gebunden.

4. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

Registerkarte „UI Options“

Verwenden Sie die Registerkarte **Administrators > Delegation >** *Rollenname* **> General > UI Options**, um die Webkonsoleneinstellungen für die Administratoren, die dieser Rolle zugewiesen sind, anzupassen (einschließlich Konsolenfarben, Logos und hierarchischer Navigationsmenüs). (Weitere Informationen über das Anpassen des Logos und der Farben der Webkonsolen-Anmeldeseite finden Sie unter „Registerkarte „Sign-in Pages““ auf Seite 204.)

Hierarchische Navigationsmenüs sind dynamische Menüs, die angezeigt werden, wenn Sie mit dem Mauszeiger auf eines der Menüs im linken Bereich der Webkonsole zeigen. Wenn Sie beispielsweise hierarchische Navigationsmenüs aktivieren und dann in der Webkonsole auf das Menü **System > Signing In** zeigen, werden die Untermenüs **Sign-In Policies**, **Sign-In Pages** und **Authentication/Authorization Servers** angezeigt. Verwenden Sie diese Menüs, um schnell im System zu navigieren, ohne sich durch die gesamte Menühierarchie klicken zu müssen.

HINWEIS:

- Informationen zu Umgebungen mit Unterstützung hierarchischer Menüs finden Sie auf der Juniper Networks-Supportsite im Dokument *IVE Supported Platforms*.
- Wenn Sie unter **Administrators** oder **Users** mehr als 10 Authentifizierungsbereiche definiert haben, zeigt die Webkonsole nur die 10 Rollen oder Bereiche der hierarchischen Navigationsmenüs an, auf die zuletzt zugegriffen wurde. Das IVE zeigt nicht die 10 Rollen und Bereiche an, auf die der aktuelle Administrator zuletzt zugegriffen hat – es zeigt die 10 Rollen und Bereiche an, auf die alle an diesem IVE angemeldeten Administratoren zugegriffen haben.

Anpassen der IVE-Willkommensseite für Benutzer mit Rollen

So passen Sie die IVE-Willkommensseite für Benutzer mit Rollen an:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Delegation >** *Rollenname*.
2. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **UI Options**, um diese Einstellungen für die Rolle zu aktivieren.
3. Wählen Sie **General > UI Options**, um Einstellungen für die Rolle anzupassen.
4. Legen Sie im Abschnitt **Header** eine benutzerdefinierte Logobilddatei und eine andere Farbe für den Seitenkopf fest.
5. Legen Sie im Abschnitt **Navigation Menus** fest, ob hierarchische Navigationsmenüs angezeigt werden sollen. Folgende Optionen stehen zur Verfügung:
   - **Auto-enabled** – Das IVE ermittelt, ob sich der Administrator von einer unterstützten Pattform aus angemeldet hat. Die hierarchischen Menüs werden entsprechend aktiviert bzw. deaktiviert.
   - **Enabled** – Das IVE aktiviert hierarchische Menüs unabhängig von Ihrer Plattform. Wenn sich ein Administrator über eine nicht unterstützte Plattform angemeldet hat, können die hierarchischen Menüs von ihm u. U. nicht verwendet werden, obwohl sie aktiviert sind.
   - **Disabled** – Das IVE deaktiviert hierarchische Menüs für alle Mitglieder der Rolle.

6. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, doch möglicherweise muss bei den aktuellen Browsersitzungen von Benutzern eine Aktualisierung durchgeführt werden, damit die Änderungen angezeigt werden. Oder klicken Sie auf **Restore Factory Defaults**, um das Erscheinungsbild der Webkonsole auf die Standardeinstellungen zurückzusetzen.

Kapitel 9

Benutzereinstellungen

Auf der Webkonsole können Sie mithilfe der Einstellungen im Abschnitt **Users** Benutzerauthentifizierungsbereiche und -rollen erstellen und konfigurieren sowie Benutzer zu einem lokalen Authentifizierungsserver hinzufügen.

Inhalt

- „Konfigurieren der Seite „Authentication““ auf Seite 275
- „Konfigurieren der Seite „Roles““ auf Seite 276
- „Konfigurieren der Seite „New User““ auf Seite 301

Konfigurieren der Seite „Authentication“

Auf der Seite **Users > Authentication** können Sie Benutzerauthentifizierungsbereiche erstellen und konfigurieren sowie Rollenzuordnungsregeln erstellen. Weitere Informationen und Anweisungen für die Konfiguration eines Administrator- und Benutzerauthentifizierungsbereichs finden Sie unter „Konfigurieren der Seite „Authentication““ auf Seite 257.

Konfigurieren der Seite „Roles“

Das Menü **Users > Roles** ist mit den Seiten **Roles** für Benutzer verknüpft. Auf dieser Seite können Sie Benutzerrollen im System erstellen und verwalten. Klicken Sie zum Erstellen einer Rolle auf **New Role**, und geben Sie dann einen Namen sowie bei Bedarf eine Beschreibung ein. Dieser Name wird auf der Seite **Roles** in der Liste **Roles** angezeigt. Klicken Sie auf den Namen der Rolle, um auf den Registerkarten **Roles** mit der Konfiguration zu beginnen.

Dieser Abschnitt enthält die folgenden Anweisungen zum Konfigurieren der Unterregisterkarten **Roles**:

- „Konfigurieren der Seite „General““ auf Seite 277 – Hier wird die Angabe von allgemeinen Rolleneinstellungen, Zugriffsverwaltungsoptionen, Benutzersitzungsoptionen und benutzerdefinierten IVE-Willkommensseiten beschrieben.

Konfigurieren der Seite „General“

Die Seite **General** enthält die folgenden Registerkarten:

- „Registerkarte „Overview““ auf Seite 277 – Auf dieser Registerkarte können Sie den Namen und die Beschreibung von Rollen bearbeiten, Sitzungs- und Benutzeroberflächenoptionen aktivieren und deaktivieren sowie Zugriffsfunktionen aktivieren.
- „Registerkarte „Restrictions““ auf Seite 278 – Auf dieser Registerkarte können Sie Zugriffsverwaltungsoptionen für die Rolle festlegen.
- „Registerkarte „Source IP““ auf Seite 278 – Auf dieser Registerkarte können Sie rollenbasierte Quell-IP-Aliasnamen festlegen.
- „Registerkarte „Session Options““ auf Seite 279 – Auf dieser Registerkarte können Sie Sitzungszeitbegrenzungen, Roamingfunktionen, die Sitzungs- und Kennwortbeständigkeit, Optionen zur Anforderungsverfolgung sowie Anwendungsaktivitäten bei Leerlaufzeitüberschreitungen festlegen.
- „Registerkarte „UI Options““ auf Seite 281 – Auf dieser Registerkarte können Sie benutzerdefinierte Einstellungen für die IVE-Willkommensseite von Benutzern festlegen, die dieser Rolle zugeordnet sind.

Registerkarte „Overview“

Auf der Registerkarte **Overview** können Sie den Namen und die Beschreibung von Rollen bearbeiten, Sitzungs- und Benutzeroberflächenoptionen aktivieren und deaktivieren sowie Zugriffsfunktionen aktivieren. Wenn Sie eine Zugriffsfunktion aktivieren, müssen Sie auch entsprechende Ressourcenrichtlinien erstellen.

Verwalten allgemeiner Einstellungen und Optionen für Rollen

So verwalten Sie allgemeine Einstellungen und Optionen für Rollen:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Ausgewählte Rolle* **> General > Overview** aus.
2. Überprüfen Sie den Namen und die Beschreibung, und klicken Sie anschließend auf **Save Changes**. (Dies ist optional.)
3. Aktivieren Sie unter **Options** folgende Kontrollkästchen:
   - **Source IP**, um die auf der Registerkarte **General > Source IP** konfigurierten Einstellungen auf die Rolle anzuwenden.
   - **Session Options**, um die auf der Registerkarte **General > Session Options** konfigurierten Einstellungen auf die Rolle anzuwenden.
   - **UI Options**, um die auf der Registerkarte **General > UI Options** konfigurierten Einstellungen auf die Rolle anzuwenden.

4. Aktivieren Sie unter **Access features** die für die Rolle vorgesehenen Funktionen.

5. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

Registerkarte „Restrictions“

Legen Sie auf der Registerkarte **Restrictions** Zugriffsverwaltungsoptionen für die Rolle fest. Das IVE berücksichtigt diese Beschränkungen, wenn es ermittelt, ob ein Benutzer einer Rolle zugeordnet wird. Benutzer werden der Rolle vom IVE nur dann zugeordnet, wenn Sie die angegebenen Beschränkungen erfüllen. Weitere Informationen zur Zugriffsverwaltung finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 38.

Festlegen von Zugriffsverwaltungsoptionen für die Rolle

So legen Sie Zugriffsverwaltungsoptionen für die Rolle fest:

1. Wählen Sie in der Webkonsole die Optionen **Users** > **Roles** > *Ausgewählte Rolle* > **General** > **Restrictions** aus.

2. Klicken Sie auf die Registerkarte der Option, die Sie für die Rolle konfigurieren möchten, und konfigurieren Sie sie gemäß den Anweisungen in den folgenden Abschnitten:

   - „Angeben von IP-Quelladresseinschränkungen“ auf Seite 418
   - „Angeben von Browsereinschränkungen“ auf Seite 419
   - „Angeben clientseitiger Zertifikateinschränkungen“ auf Seite 421
   - „Angeben von Host Checker-Einschränkungen“ auf Seite 423
   - „Angeben von Cache Cleaner-Einschränkungen“ auf Seite 425

   Für die Rolle kann eine beliebige Anzahl von Zugriffsverwaltungsoptionen konfiguriert werden. Wenn ein Benutzer nicht alle Beschränkungen erfüllt, ordnet das IVE ihn der Rolle nicht zu.

Registerkarte „Source IP“

Festlegen von Quell-IP-Aliasen für die Rolle

So legen Sie einen Quell-IP-Alias für die Rolle fest:

1. Wählen Sie in der Webkonsole die Optionen **Users** > **Roles** > *Ausgewählte Rolle* > **General** > **Source IP** aus.

2. Wählen Sie im Dropdownmenü eine Quell-IP-Adresse aus.

3. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

HINWEIS:

- Wenn ein Endbenutzer mehreren Rollen zugeordnet ist und das IVE Rollen zusammenführt, ordnet das IVE die für die erste Rolle konfigurierte Quell-IP-Adresse in der Liste der zusammengeführten Rolle zu.
- Eine Quell-IP-Adresse kann für mehrere Rollen angegeben werden. Es ist jedoch nicht möglich, mehrere Quell-IP-Adressen für eine Rolle anzugeben.

Registerkarte „Session Options“

Auf der Registerkarte **Session** können Sie Sitzungszeitbegrenzungen, Roamingfunktionen, die Sitzungs- und Kennwortbeständigkeit, Optionen zur Anforderungsverfolgung sowie Anwendungsaktivitäten bei Leerlaufzeitüberschreitungen festlegen. Aktivieren Sie auf der Registerkarte **Overview** das Kontrollkästchen **Session Options**, um diese Einstellungen für die Rolle zu aktivieren.

Optionen für Benutzersitzungen festlegen

So legen Sie allgemeine Sitzungsoptionen fest:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Ausgewählte Rolle* **> General > Session Options** aus.
2. Geben Sie unter **Session Lifetime** Werte für folgende Optionen an:
   - **Idle Timeout** – Geben Sie die Anzahl der Minuten an, die sich eine nicht administrative Benutzersitzung im Leerlauf befinden kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Leerlaufzeitbegrenzung für Sitzungen beträgt in der Standardeinstellung zehn Minuten, d. h., eine Benutzersitzung, die zehn Minuten lang inaktiv ist, wird vom IVE beendet, und das Ereignis wird im Systemprotokoll protokolliert (sofern Sie nicht die unten beschriebenen Warnungen bei Sitzungszeitüberschreitung aktivieren).
   - **Max. Session Length** – Geben Sie die Anzahl der Minuten an, die eine aktive nicht administrative Benutzersitzung geöffnet bleiben kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Standardzeitbegrenzung für eine Benutzersitzung beträgt sechzig Minuten. Nach dieser Zeitspanne beendet das IVE die Benutzersitzung und protokolliert das Ereignis im Systemprotokoll.
   - **Reminder Time** – Geben Sie den Zeitpunkt an, zu dem das IVE Benutzer (außer Administratoren) wegen einer bevorstehenden Sitzungs- oder Leerlaufzeitüberschreitung warnen soll. Geben Sie die Anzahl von Minuten vor Erreichen der Überschreitung an.

3. Aktivieren Sie unter **Enable Session timeout warning** das Optionsfeld **Enabled**, um vor dem Erreichen der Sitzungszeitbegrenzung oder des Leerlaufzeitlimits auch andere Benutzer als Administratoren zu benachrichtigen. In diesen Warnungen werden Benutzer aufgefordert, kurz vor Erreichen der Sitzungsbegrenzung oder des Leerlaufzeitlimits eine geeignete Aktion durchzuführen, um gerade in Verarbeitung befindliche Formulardaten speichern zu können, die andernfalls verloren gehen würden. Benutzer, die sich dem Leerlaufzeitlimit nähern, werden zum Reaktivieren der Sitzung aufgefordert. Benutzer, die sich der Sitzungszeitbegrenzung nähern, werden zum Speichern der Daten aufgefordert.

4. Geben Sie unter **Roaming session** Folgendes an:

   - **Enabled** – Ermöglicht Roamingbenutzersitzungen für Benutzer, die dieser Rolle zugeordnet sind. Eine Roamingbenutzersitzung funktioniert über Quell-IP-Adressen, wodurch sich mobile Benutzer (Benutzer von Laptops) mit dynamischen IP-Adressen von einem Standort aus beim IVE anmelden können und Ihre Arbeit von einem anderen Standort fortsetzen können. Einige Browser weisen jedoch eventuell Schwachstellen auf, über die durch bösartigen Code Benutzercookies gestohlen werden können. Ein böswilliger Benutzer kann dann ein gestohlenes IVE-Sitzungscookie verwenden, um sich beim IVE anzumelden.

   - **Limit to subnet** – Beschränkt die Roamingsitzung auf das lokale Subnetz, das im Feld **Netmask** angegeben ist. Benutzer können sich von einer IP-Adresse aus anmelden und ihre Sitzungen mit einer anderen IP-Adresse fortsetzen, sofern sich die neue IP-Adresse in demselben Subnetz befindet.

   - **Disabled** – Verbietet Roamingbenutzersitzungen für Benutzer, die dieser Rolle zugeordnet sind. Benutzer, die sich von einer IP-Adresse aus anmelden, können eine aktive IVE-Sitzung nicht von einer anderen IP-Adresse aus fortsetzen. Benutzersitzungen sind an die ursprüngliche Quell-IP-Adresse gebunden.

5. Aktivieren Sie unter **Persistent session** das Optionsfeld **Enabled**, um das IVE-Sitzungscookie auf die Festplatte des Clients zu schreiben, sodass die Anmeldeinformationen des IVE-Benutzers für die Dauer der IVE-Sitzung gespeichert werden.

   Standardmäßig wird das IVE-Sitzungscookie aus dem Speicher des Browsers gelöscht, wenn der Browser geschlossen wird. Die IVE-Sitzungsdauer wird sowohl vom Wert des Leerlaufzeitlimits als auch dem Wert der Höchstsitzungsdauer bestimmt, die Sie für die Rolle angeben. Die IVE-Sitzung wird nicht beendet, wenn ein Benutzer den Browser schließt. Eine IVE-Sitzung wird erst dann beendet, wenn sich ein Benutzer vom IVE abmeldet. Wenn ein Benutzer das Browserfenster schließt, ohne sich abzumelden, kann jeder beliebige Benutzer eine andere Instanz desselben Browsers öffnen, um auf das IVE zuzugreifen, ohne gültige Anmeldeinformationen zu senden.

HINWEIS: Wir empfehlen, diese Funktion nur für Rollen zu aktivieren, deren Mitglieder den Zugriff auf Anwendungen benötigen, für die IVE-Anmeldeinformationen erforderlich sind. Zudem sollten Sie dafür sorgen, dass sich diese Benutzer der Bedeutung der Abmeldung vom IVE nach Abschluss der Sitzung bewusst sind.

6. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

Registerkarte „UI Options“

Auf der Registerkarte **UI Options** können Sie benutzerdefinierte Einstellungen für die IVE-Willkommensseite von Benutzern angeben, die dieser Rolle zugeordnet sind. Die IVE-Willkommensseite (oder Startseite) ist die Weboberfläche, die authentifizierten IVE-Benutzern angezeigt wird. Aktivieren Sie auf der Registerkarte **Overview** das Kontrollkästchen **UI Options**, um benutzerdefinierter Einstellungen für die Rolle zu aktivieren. Andernfalls verwendet das IVE die Standardeinstellungen.

Anpassen der IVE-Willkommensseite für Benutzer mit Rollen

So passen Sie die IVE-Willkommensseite für Benutzer mit Rollen an:

1. Wählen Sie **Users > Roles >** *Ausgewählte Rolle* **> General > UI Options**.

2. Legen Sie unter **Header** ein benutzerdefiniertes Logo und eine alternative Hintergrundfarbe für den Kopfbereich der IVE-Willkommensseite fest (optional):

   - Klicken Sie auf die Schaltfläche **Browse**, und machen Sie die benutzerdefinierte Bilddatei ausfindig. Im Fenster **Current appearance** wird das neue Logo erst dann angezeigt, wenn Sie Ihre Änderungen gespeichert haben.

   - Geben Sie die Hexadezimalzahl für die Hintergrundfarbe ein, oder klicken Sie auf das Symbol **Color Palette**, und wählen Sie die gewünschte Farbe aus. Das Fenster **Current appearance** wird darauf aktualisiert.

3. Wählen Sie unter **Sub-headers** neue Hintergrund- und Textfarben aus (optional):

   - Geben Sie die Hexadezimalzahl im Feld **Background color** ein, oder klicken Sie auf das Symbol **Color Palette**, und wählen Sie die gewünschte Farbe aus. Das Fenster **Current appearance** wird darauf aktualisiert.

   - Geben Sie die Hexadezimalzahl im Feld **Text color** ein, oder klicken Sie auf das Symbol **Color Palette**, und wählen Sie die gewünschte Farbe aus. Das Fenster **Current appearance** wird darauf aktualisiert.

4. Ordnen Sie unter **Bookmarks Panel Arrangement** die Fenster so an, wie sie auf der Lesezeichenseite des Benutzers angezeigt werden sollen:

   a. Markieren Sie den Namen eines Fensters in der Liste **Left Column** oder **Right Column**.

   b. Wenn Sie das Fenster über oder unter den anderen Fenstern positionieren möchten, klicken Sie auf **Move Up** bzw. **Move Down.**

   c. Wenn Sie das Fenster auf die andere Seite der Lesezeichenseite des Benutzers verschieben möchten, klicken Sie auf **Move >** oder **< Move**.

d. Wenn Sie die Standardanordnung verwenden möchten, klicken Sie auf **Reset to default**.

HINWEIS: Das IVE zeigt alle Fenster unter **Bookmarks Panel Arrangement** für alle lizenzierten Funktionen an, unabhängig davon, ob Sie die entsprechende Funktion oder Rolle aktivieren.

5. Wählen Sie unter **User toolbar** Optionen für die Symbolleiste auf der IVE-Lesezeichenseite und anderen sicheren Gatewayseiten auf dem IVE aus:

   - **Preferences** – Bei Auswahl dieser Option wird die Schaltfläche **Preferences** angezeigt.

   - **Session Counter** – Bei Auswahl dieser Option wird ein Zeitwert auf der Benutzersymbolleiste angezeigt, der die maximal verbleibende Zeit in der aktuellen Sitzung des Benutzers angibt. Die aktuelle Sitzung kann noch vor Ablauf dieser maximalen Zeit beendet werden, wenn über einen bestimmten Zeitraum keine Benutzeraktivität stattfindet.

   - **Client Application Sessions** – Bei Auswahl dieser Option wird die Schaltfläche **Client Apps** auf der Benutzersymbolleiste angezeigt. Über diese Schaltfläche können Benutzer die Seite **Client Application Sessions** aufrufen, auf der Sie Clientanwendungen wie Network Connect oder Secure Application Manager starten können. Wenn Sie diese Option nicht auswählen, zeigt das IVE das Fenster **Client Application Sessions** auf der IVE-Lesezeichenseite an.

6. Legen Sie unter **Personalized greeting** eine Begrüßungs- und Benachrichtigungsmeldung für die IVE-Lesezeichenseite fest (optional):

   - **Enable** – Wählen Sie diese Option aus, um die persönliche Begrüßung anzuzeigen. Das IVE zeigt den Benutzernamen an, wenn der vollständige Name nicht konfiguriert wurde.

   - Wählen Sie **Show notification message**, und geben Sie einen Meldungstext in das entsprechende Textfeld ein (optional). Die Meldung wird oben auf der IVE-Lesezeichenseite angezeigt, nachdem Sie die Änderungen gespeichert haben und der Benutzer diese Seite aktualisiert. Sie können die folgenden HTML-Tags verwenden, um den Text zu formatieren und Links hinzuzufügen: <i>, <b>, <br>, <font> und <a href>. Allerdings schreibt das IVE Verknüpfungen auf der Anmeldseite (aufgrund der noch nicht erfolgten Benutzerauthentifizierung) nicht neu. Folglich sollten Sie nur Verweise auf externe Sites erstellen. Verknüpfungen zu Sites hinter einer Firewall funktionieren nicht.

HINWEIS: Wenn Sie in der benutzerdefinierten Meldung nicht unterstützte HTML-Tags verwenden, zeigt das IVE die IVE-Startseite des Benutzers möglicherweise nicht korrekt an.

7. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, doch möglicherweise muss bei den aktuellen Browsersitzungen von Benutzern eine Aktualisierung durchgeführt werden, damit die Änderungen angezeigt werden.

8. Klicken Sie auf **Restore Factory Defaults**, um alle Optionen für die Benutzeroberfläche auf die Standardeinstellungen zurückzusetzen (dies ist optional).

Konfigurieren der Seite „Web“

Die Seite **Web** enthält die folgenden Registerkarten:

- „Registerkarte „Bookmarks““ auf Seite 284 – Diese Registerkarte dient zum Erstellen von Lesezeichen für Webressourcen.
- „Registerkarte „Options““ auf Seite 287 – Diese Registerkarte dient zum Festlegen allgemeiner Webbrowsingoptionen.

Registerkarte „Bookmarks“

Auf der Registerkarte **Bookmarks** können Sie Lesezeichen erstellen, die für dieser Rolle zugeordnete Benutzer auf der Willkommensseite angezeigt werden. Über diese Seite können zwei Lesezeichentypen erstellt werden:

- **Lesezeichen für Web-URLs** – Diese Lesezeichen sind Links zu Web-URLs im World Wide Web oder im Firmenintranet. Sie können beim Erstellen von Weblesezeichen den IVE-Benutzernamen eines Benutzers im URL-Pfad einfügen, um Single Sign-on-Zugriff auf Back-End-Webanwendungen zu ermöglichen. Anweisungen für die Konfiguration von Weblesezeichen finden Sie unter „Erstellen von Lesezeichen für Web-URLs“ auf Seite 284.
- **Lesezeichen für Java-Applets** – Diese Lesezeichen sind Links zu Java-Applets, die über die Seite **Resource Policies > Web > Java > Applets** der Webkonsole in das IVE hochgeladen werden. Anweisungen für die Konfiguration von Lesezeichen für Java-Applets finden Sie unter „Erstellen von Lesezeichen für Java-Applets“ auf Seite 285.

Wenn Sie einen dieser Lesezeichentypen erstellen, werden die entsprechenden Links auf der Willkommensseite der Benutzer angezeigt, die dieser Rolle zugeordnet sind.

Erstellen von Lesezeichen für Web-URLs

So erstellen Sie ein Lesezeichen für eine Webressource:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Rollenname* **> Web > Bookmarks**.
2. Klicken Sie auf **New Bookmark**.
3. Geben Sie einen Namen und eine Beschreibung für das Lesezeichen ein (optional). Diese Informationen werden anstelle des URLs auf der IVE-Startseite angezeigt.
4. Wählen Sie **Web URL** aus.
5. Geben Sie den URL für das Lesezeichen ein. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im URL <username> ein.

6. Klicken Sie unter **Auto-allow** auf **Auto-allow Bookmark**, damit das IVE automatisch eine entsprechende Ressourcenrichtlinie für den Webzugriff erstellen kann. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt. Wählen Sie anschließend folgende Option aus:

   - **Only this URL**, um Benutzern nur den Zugriff auf den URL zu gestatten.
   - **Everything under this URL**, um Benutzern den Zugriff auf alle Pfade unter diesem URL zu gestatten.

7. Klicken Sie unter **Display options** auf **Open bookmark in a new window**, um dem IVE das automatische Öffnen der Webressource in einem neuen Browserfenster zu ermöglichen. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt. Wählen Sie anschließend folgende Option aus:

   - **Do not display the URL address bar**, wenn die Adresszeile aus dem Browserfenster entfernt werden soll. Diese Funktion veranlasst die Weiterleitung des gesamten Webdatenverkehrs über das IVE, indem verhindert wird, dass Benutzer in der angegebenen Rolle einen neuen URL in die Adresszeile eingeben, durch den das IVE umgangen wird.
   - **Do not display the menu and the toolbar**, um das Menü und die Symbolleiste aus dem Browser zu entfernen. Diese Funktion entfernt Menüs, Browserschaltflächen und Lesezeichen aus dem Browserfenster, um nur das Browsen über das IVE zu ermöglichen.

8. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

Erstellen von Lesezeichen für Java-Applets

So erstellen Sie ein Lesezeichen für ein Java-Applet im IVE:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Rollenname* **> Web > Bookmarks**.
2. Klicken Sie auf **New Bookmark**.
3. Geben Sie einen Namen (erforderlich) und eine Beschreibung (optional) für das Lesezeichen ein. Diese Informationen werden auf der IVE-Startseite angezeigt.
4. Wählen Sie **Java Applet** aus.
5. Wählen Sie in der Liste **Applet/Code** die Java-Applets aus, auf die in dieser Webseite verwiesen werden soll. Das IVE füllt diese Liste mit den Java-Applets auf, die Sie über die Seite **Resource Policies > Web > Java > Applets** der Webkonsole hochladen.
6. Klicken Sie auf **Generate HTML**, um eine HTML-Seitendefinition mit Verweisen auf die Java-Applets zu erstellen. Geben Sie anschließend die erforderlichen Attribute und Parameter anhand der Richtlinien in den folgenden Abschnitten ein:

- „Erforderliche Attribute für hochgeladene Java-Applets“ auf Seite 286
- „Erforderliche Parameter für hochgeladene Java-Applets“ auf Seite 287

Sie können auch zusätzlichen HTML-Code oder JavaScript für diese Webseitendefinition hinzufügen. Das IVE schreibt den gesamten in diesem Feld eingegebenen Code neu.

HINWEIS: In diesem Feld dürfen keine relativen Links zu URLs oder Dokumenten hinzugefügt werden. Andernfalls schlagen diese Links fehl, wenn der Benutzer versucht, über die IVE-Endbenutzerkonsole auf die Links zuzugreifen.

7. Klicken Sie unter **Display options** auf **Open bookmark in a new window**, um dem IVE das automatische Öffnen der Webressource in einem neuen Browserfenster zu ermöglichen. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt. Wählen Sie anschließend folgende Option aus:
   - **Do not display the URL address bar**, wenn die Adresszeile aus dem Browserfenster entfernt werden soll. Diese Funktion veranlasst die Weiterleitung des gesamten Webdatenverkehrs über das IVE, indem verhindert wird, dass Benutzer in der angegebenen Rolle einen neuen URL in die Adresszeile eingeben, durch den das IVE umgangen wird.
   - **Do not display the menu and the toolbar**, um das Menü und die Symbolleiste aus dem Browser zu entfernen. Diese Funktion entfernt Menüs, Browserschaltflächen und Lesezeichen aus dem Browserfenster, um nur das Browsen über das IVE zu ermöglichen.
8. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

Erforderliche Attribute für hochgeladene Java-Applets

Wenn Sie ein Lesezeichen für Java-Applets über das IVE erstellen, müssen Sie die folgenden Attribute und entsprechenden Werte definieren. Bei Verwendung der Funktion **Generate HTML** füllt das IVE einige dieser Informationen für Sie aus, und es fügt den von Ihnen zu definierenden Attributen den Zusatz PLEASE_SPECIFY hinzu. Verwenden Sie zum Angeben von Attributen und zugehörigen Werten das Format *attribute="value"*. Folgende Attribute sind erforderlich:

- **code** – Gibt die im Java-Applet aufzurufende Klassendatei an. Verwenden Sie diesen Wert, um auf die Hauptfunktion des Java-Applets zu verweisen. Beispiel:

  ```
  applet code="com.citrix.JICA"
  ```

- **codebase** – Gibt an, von wo der Webbrowser das Applet abrufen kann. Verwenden Sie die Variable <<CODEBASE>>, die auf den Speicherort auf dem IVE verweist, an dem das IVE das Java-Applet speichert. Beispiel:

  ```
  codebase="<< CODEBASE >>"
  ```

- **archive** – Gibt an, welche Archivdateien (d. h. jar-, .cab- oder .zip-Dateien) der Webbrowser abrufen soll. Wenn Sie mehrere Werte für dieses Attribut angeben, trennen Sie sie durch Kommas. Beispiel:

  archive="JICAEngN.jar,JICA-sicaN.jar,cryptojN.jar,JICA-configN.jar,JICA-coreN.jar"

- **width und height** – Geben die Größe des Java-Appletfensters an (optional). Beispiel:

  width="640" height="480"

- **name** – Gibt eine Beschriftung für das Java-Applet an (optional). Beispiel:

  name="CitrixJICA"

- **align** – Gibt die Ausrichtung das Java-Appletfensters im Browserfenster an (optional). Beispiel:

  align="top"

Erforderliche Parameter für hochgeladene Java-Applets

Wenn Sie Lesezeichen für Java-Applets über das IVE erstellen, müssen Sie Parameter und Werte definieren, die das IVE an das Java-Applet übergeben soll. Diese Parameter sind appletspezifisch. Verwenden Sie zum Festlegen von Parametern und zugehörigen Werten das folgende Format:

<param name="Parametername" value="Wertname">

Mit Ausnahme von Parametername und Wertname handelt es sich bei dem gesamten Text um Literalzeichen.

Werte können mithilfe von IVE-Variablen an das Java-Applet übergeben werden. Schließen Sie die Variablennamen hierzu in doppelte Klammern ein. Sie können z. B. die Werte <<username>> und <<password>> an das Java-Applet übergeben. Eine Liste der verfügbaren IVE-Variablen finden Sie unter „Systemvariablen und Beispiele“ auf Seite 401.

Wenn Sie eine Webseite mit einem für Sie geeigneten Demo-Applet finden, rufen Sie die Demosite auf, und zeigen Sie den Quellcode auf der Seite an, die das Java-Applet ausführt. Suchen Sie im Quellcode nach dem Tag applet. Machen Sie das Attribut code im Quellecode ausfindig, und überprüfen Sie, ob es spezielle Parameter enthält, die an den Browser übergeben werden müssen. In den meisten Fällen können das Attribut code und die entsprechenden Parameter kopiert und direkt in das HTML-Feld für Ihr IVE-Lesezeichen eingefügt werden. Wenn ein Parameter jedoch eine Ressource auf dem lokalen Webserver referenziert, kann der Verweis nicht kopiert und in das IVE-Lesezeichen eingefügt werden, da das IVE keinen Zugriff auf die lokalen Ressourcen des anderen Webservers hat. Überprüfen Sie beim Kopieren/Einfügen von Parametern aus einer anderen Quelle immer die Werte der Parameter.

Registerkarte „Options“

Auf der Registerkarte **Options** können Sie allgemeine Webbrowsingoptionen festlegen.

Angeben von allgemeinen Webbrowsingoptionen

So geben Sie allgemeine Webbrowsingoptionen an:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Rollenname* **> Web > Options**.

2. Geben Sie unter **Browsing** die Optionen an, die für Benutzer aktiviert werden sollen:

   - **User can type URLs in IVE browse bar** – Diese Option ermöglicht es Benutzern, auf der Willkommensseite URLs einzugeben und Sites im Internet aufzurufen.

   - **Allow Java applets** – Diese Option ermöglicht es Benutzern, Webseiten aufzurufen, die clientseitige Java-Applets enthalten. Der IVE-Server wird für den Anwendungsserver wie ein Browser über SSL behandelt. Das IVE verarbeitet alle durch ein Java-Applet initiierten HTTP-Anforderungen und TCP-Verbindungen transparent und verarbeitet signierte Java-Applets.

     Wenn Sie diese Funktion aktivieren, können die Benutzer Java-Applets starten und Anwendungen ausführen, die als clientseitige Java-Applets implementiert wurden, z. B. VNC-Java-Client (Virtual Computing), Citrix NFuse Java-Client, WRQ Reflections Web-Client und Lotus WebMail. Diese Funktion wird zusammen mit den Ressourcenrichtlinien für die Java-Codesignatur verwendet. Weitere Informationen finden Sie unter „Registerkarte „Code Signing““ auf Seite 317.

   - **Allow Flash content** – Wenn diese Option aktiviert ist, vermittelt das IVE Flash-Inhalt über sein Modul für die Inhaltsvermittlung. Das IVE bietet beschränkte Unterstützung für ActionScript 2.0 und Flash Remoting und unterstützt keine XMLSocket-Verbindungen.

   - **Mask hostnames while browsing** – Bei Auswahl dieser Option werden Zielressourcen im URL verborgen, die von Benutzern aufgerufen werden können. Wenn Sie die Option auswählen, werden die IP-Adressen und Hostnamen für den Benutzer an folgenden Stellen maskiert:

     - Adressleiste des Webbrowsers (wenn der Benutzer eine Seite aufruft)

     - Statusleiste des Webbrowsers (beim Führen des Mauszeigers über einen Hyperlink)

     - HTML-Quelldateien (wenn der Benutzer „View Source“ auswählt)

     Durch die Hostnamencodierung (auch bezeichnet als Hostnamenverschleierung oder URL-Verschleierung) wird verhindert, dass sich zufällige Besucher den URL einer internen Ressource notieren können. Zu diesem Zweck wird der Zielserver innerhalb des URL verborgen, ohne dass dabei der vollständige Pfadname, die Zieldatei oder die Portnummer maskiert werden. Wenn ein Benutzer z B. www.msn.com aufruft und das selektive Neuschreiben oder die Hostnamencodierung nicht aktiviert ist, wird der folgende URL in der Adressleiste des Webbrowsers angezeigt: http://www.msn.com/.

Wenn das selektive Neuschreiben aktiviert ist, zeigt das IVE möglicherweise den folgenden URL an:

https://10.10.9.1/,DanaInfo=www.msn.com+

Wenn die Hostnamencodierung anschließend aktiviert wird und derselbe Benutzer diese Site aufruft, wird ein URL mit verborgenem Hostnamen (www.msn.com) angezeigt:

https://10.10.9.1/,DanaInfo=.awxyCqxtGkxw+

Bei der Hostnamencodierung wird ein umkehrbarer Lightweight-Algorithmus verwendet, so dass Benutzer codierte URLs als Lesezeichen festlegen können. (Das IVE kann den codierten URL übersetzen und wieder in den ursprünglichen URL auflösen.) Aus Kompatibilitätsgründen funktionieren zuvor erstellte Lesezeichen für nicht maskierte URLs auch nach der Aktivierung der Hostnamencodierung.

Wenn Sie bei aktivierter Option das selektive Neuschreiben und die Hostnamencodierung aktivieren, maskiert das IVE nur die Hostnamen und IP-Adressen der ausgewählten, mit der Option für das selektive Umschreiben umzuschreibenden Server. Hostnamen und IP-Adressen werden in Protokolleinträgen nicht maskiert. Dies gilt auch für Protokolleinträge zur Hostnamencodierung.

- **Unrewritten pages open in new window** – Wenn Benutzer auf Seiten zugreifen, die nicht neu geschrieben werden (siehe „Schreiben einer Ressourcenrichtlinie für selektives Neuschreiben“ auf Seite 321), erzwingt diese Option, dass der Inhalt in einem neuen Fenster angezeigt wird. So werden Benutzer daran erinnert, dass sie sich noch immer in einer sicheren Sitzung befinden. Wenn ein Benutzer eine Ressource anfordert, auf die diese Option zutrifft, zeigt das IVE eine Seite an, die eine Verknüpfung mit der angeforderten Ressource enthält, und der Benutzer wird aufgefordert, auf diese Verknüpfung zu klicken. Durch diese Verknüpfung wird die Ressource in einem neuen Browserfenster geöffnet, und die Seite, von der die Anforderung stammt, wird weiterhin im IVE angezeigt.

  Wenn Sie dieses Kontrollkästchen deaktivieren, bemerken die Benutzer möglicherweise nicht, dass ihre IVE-Sitzung noch aktiv ist und sie im Browser auf die Schaltfläche **Zurück** klicken müssen, um zum IVE zurückzukehren. Zum Abmelden müssen die Benutzer zum IVE zurückkehren. Wenn sie lediglich das Browserfenster schließen, bleiben die Sitzungen bis zum Ablaufen der Sitzungszeitbegrenzung aktiv.

- **Allow browsing untrusted SSL web servers** – Wenn diese Option aktiviert ist, können Benutzer über das IVE auf nicht vertraute Websites zugreifen. Nicht vertraute Websites sind Sites, deren Serverzertifikate nicht über die Registerkarte **System > Configuration > Certificates > Trusted Servers CAs** der Webkonsole installiert werden. Weitere Informationen finden Sie unter „Registerkarte „Trusted Server CAs““ auf Seite 179. Bei Auswahl dieser Option können Sie festlegen, welche Auswahlmöglichkeiten das IVE Benutzern bereitstellt, wenn sie eine nicht vertraute Website aufrufen:

- **Warn users about the certificate problems** – Wenn diese Option aktiviert ist, zeigt das IVE einen Warnhinweis an, wenn der Benutzer zum ersten Mal auf eine nicht vertraute Website zugreift. Der Benutzer wird darüber informiert, weshalb dem Zertifikat der Website nicht vertraut wird, und er hat die Möglichkeit, den Vorgang fortzusetzen oder abzubrechen. Entscheidet sich der Benutzer fortzufahren, nachdem das IVE einen Warnhinweis angezeigt hat, zeigt das IVE während der aktuellen IVE-Sitzung keine weiteren Warnhinweise zu dieser Website an.

HINWEIS: Wenn Sie die Option **Warn users about the certificate problems** auswählen und der Benutzer auf Nicht-HTML-Inhalte zugreift (z. B. Bilder, js- und css-Dateien), die von einem anderen SSL-Server verarbeitet werden als die HTML-Seite, wird die Seite mit den Links u. U. nicht korrekt angezeigt. Sie können dieses Problem umgehen, indem Sie diese Option deaktivieren oder ein gültiges SSL-Produktionszertifikat auf die Server laden, die Nicht-HTML-Inhalte verarbeiten.

- **Allow users to bypass warnings on a server-by-server basis** – Wenn diese Option aktiviert ist, erlaubt das IVE dem Benutzer, alle weiteren Warnhinweise zu einer nicht vertrauten Website zu unterdrücken. Aktiviert ein Benutzer diese Option, wird für diese Website kein Warnhinweis mehr angezeigt, vorausgesetzt, der Zugriff erfolgt über das aktuelle IVE oder über ein Cluster.

HINWEIS: Wurde einem Benutzer erlaubt, auf nicht vertraute Websites zuzugreifen, ohne dass ein Warnhinweis eingeblendet wird, fügt das IVE dem Benutzerzugriffsprotokoll trotzdem einen Eintrag hinzu, wenn der Benutzer zu einer nicht vertrauten Site navigiert. Unterdrückt ein Benutzer Warnhinweise, kann er die permanenten Einstellungen der nicht vertrauten Websites mit der Option **Delete Passwords** auf der Registerkarte **System > Preferences > Advanced** der Endbenutzerkonsole löschen.

- **Rewrite file:// URLs** – Wenn diese Option aktiviert ist, schreibt das IVE die Datei://-URLs neu, so dass sie über die IVE-Dateinavigations-CGI geroutet werden.

3. Wählen Sie unter **Bookmarks** die Option **User can add bookmarks** aus, damit Benutzer auf der IVE-Willkommensseite persönliche Weblesezeichen erstellen können.

4. Aktivieren Sie unter **Cookies** die Option **Persistent cookies**, sodass Benutzer, die zu dieser Rolle gehören, ihre Browserumgebung durch Beibehaltung permanenter Cookies anpassen können. Standardmäßig löscht der IVE Webcookies, die während einer Benutzersitzung gespeichert wurden. Bei Aktivierung dieser Option können Benutzer Cookies über die Seite **Advanced Preferences** löschen.

5. Akzeptieren Sie unter **Web Applications** den Standardwert, oder legen Sie die Dauer für **HTTP Connection Timeout** fest, um dem IVE mitzuteilen, wie lange vor dem Trennen der Verbindung auf eine Antwort vom HTTP-Server gewartet werden soll. Geben Sie einen Wert zwischen 30 und 1800 Sekunden an.

HINWEIS: Bei einem höheren Zeitüberschreitungswert, werden u. U. IVE-Ressourcen beansprucht, wenn Anwendungen Verbindungen nicht korrekt beenden oder zum Trennen der Verbindungen zu viel Zeit benötigen. Verwenden Sie den Standardwert, wenn eine Anwendung keinen höheren Zeitüberschreitungswert erfordert.

6. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „Files“

Die Seite **Files** enthält die folgenden Registerkarten:

- „Registerkarte „Web Bookmarks““ auf Seite 292 – Auf dieser Registerkarte können Sie Windows-Lesezeichen erstellen, die für dieser Rolle zugeordnete Benutzer auf der Willkommensseite angezeigt werden.
- „Registerkarte „UNIX Bookmarks““ auf Seite 293 – Auf dieser Registerkarte können Sie UNIX/NFS-Lesezeichen erstellen, die auf der IVE-Startseite angezeigt werden.
- „Registerkarte „Options““ auf Seite 294 – Auf dieser Registerkarte können Sie die Optionen zum Durchsuchen von Windows- und UNIX/NFS-Netzwerken angeben. Dies beinhaltet auch die Möglichkeit, Ressourcen anzuzeigen und Ordnerlesezeichen zu erstellen.

Registerkarte „Web Bookmarks“

Auf der Registerkarte **Windows Bookmarks** können Sie Windows-Lesezeichen erstellen, die für dieser Rolle zugeordnete Benutzer auf der Willkommensseite angezeigt werden. Sie können den IVE-Benutzernamen des Benutzers in den URL-Pfad einfügen, um so einen schnellen Zugriff auf die Netzwerkverzeichnisse des Benutzers zu ermöglichen.

Wenn IVE-Benutzer Dateien auf einem Dfs-Server durchsuchen, gibt der Dfs-Server anhand der in Active Directory gespeicherten Site-Konfigurationsdaten Dfs-Verweise in der richtigen Reihenfolge an das IVE zurück. Verweise auf nähere Servers befinden sich in der Liste an einer höheren Position als Verweise auf weiter entfernte Server. Die Clients durchlaufen die Verweise in der Reihenfolge, in der diese empfangen werden. Wenn eine Anforderung von einem Client eingeht, der sich in einem nicht in der Liste aufgeführten Subnetz befindet, besitzt der Server keine Informationen über den Standort des Clients und gibt die Verweise in zufälliger Reihenfolge zurück. Auf diese Weise greifen Dfs-Anforderungen vom IVE (in diesem Falle in der Rolle des Clients) möglicherweise auf einen wesentlich weiter entfernten Server zu. Dies wiederum kann zu erheblichen Verzögerungen führen, insbesondere wenn das IVE versucht, auf einen Server zuzugreifen, der aus dem Subnetz mit dem IVE nicht erreichbar ist. Wenn das IVE in einem Subnetz installiert ist, das sich nicht in der Liste des Dfs-Servers befindet, kann der Dfs-Administrator das Subnetz mit dem IVE auf dem Domänencontroller mit dem Tool „Active Directory-Standorte und -Dienste“ zur entsprechenden Site hinzufügen.

Erstellen von Lesezeichen für Windows-Ressourcen

So erstellen Sie ein Lesezeichen für eine Windows-Ressource:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Rollenname* **> Files > Windows Bookmarks**.

2. Klicken Sie auf **New Bookmark** , und wechseln Sie dann zum Server und Freigabenamen, bzw. geben Sie diesen ein. Geben Sie einen Pfad ein, um den Zugriff weiter einzuschränken. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im Pfad <Benutzername> ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des Servers/der Freigabe auf der IVE-Startseite angezeigt.

HINWEIS: Ein Windows-Server kann nicht mit einem Lesezeichen versehen werden. Sie müssen sowohl den Server- als auch den Freigabenamen angeben.

3. Wählen Sie für **Appearance** eine der folgenden Optionen aus:

   - **Appear as bookmark on homepage and in file browsing** – Das Lesezeichen wird dem Benutzer sowohl auf der Willkommensseite als auch beim Navigieren durch Netzwerkdateien angezeigt.

   - **Appear in file browsing only** – Das Lesezeichen wird dem Benutzer nur beim Navigieren durch Netzwerkdateien angezeigt.

4. Bei **Access** klicken Sie auf **Enable auto-allow access to this bookmark**, wenn das IVE automatisch eine entsprechende Ressourcenrichtlinie für Windows-Zugriff erstellen soll. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt. Wählen Sie anschließend folgende Option aus:

   - **Read-write access**, damit Benutzer Dateien auf dem Server speichern können. Benutzer können nur Dateien bis zu einer Größe von 500 MB auf den Server hochladen.

   - **Include sub-folders**, damit Benutzer Dateien in den Verzeichnissen unter dem angegebenen Lesezeichenpfad anzeigen können.

5. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

Registerkarte „UNIX Bookmarks“

Auf der Registerkarte **UNIX Bookmarks** können Sie UNIX/NFS-Lesezeichen erstellen, die auf der IVE-Startseite angezeigt werden. Sie können den IVE-Benutzernamen des Benutzers in den URL-Pfad einfügen, um so einen schnellen Zugriff auf die Netzwerkverzeichnisse des Benutzers zu ermöglichen.

Erstellen von Lesezeichen für UNIX-Ressourcen

So erstellen Sie ein Lesezeichen für eine UNIX/NFS-Ressource:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Rollenname* **> Files > UNIX Bookmarks**.

2. Klicken Sie auf **New Bookmark**, und geben Sie den Hostnamen oder die IP-Adresse des Servers und den Pfad der Freigabe ein. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im Pfad <Benutzername> ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des Servers/des Pfades auf der IVE-Startseite angezeigt.

3. Wählen Sie für **Appearance** eine der folgenden Optionen aus:

   - **Appear as bookmark on homepage and in file browsing** – Das Lesezeichen wird dem Benutzer sowohl auf der Willkommensseite als auch beim Navigieren durch Netzwerkdateien angezeigt.

   - **Appear in file browsing only** – Das Lesezeichen wird dem Benutzer nur beim Navigieren durch Netzwerkdateien angezeigt.

4. Bei **Access** klicken Sie auf **Enable auto-allow access to this bookmark**, wenn das IVE automatisch eine entsprechende UNIX/NFS-Ressourcenrichtlinie erstellen soll. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt. Wählen Sie anschließend folgende Option aus:

   - **Read-write access**, damit Benutzer Dateien auf dem Server speichern können. Benutzer können nur Dateien bis zu einer Größe von 500 MB auf den Server hochladen.

   - **Include sub-folders**, damit Benutzer Dateien in den Verzeichnissen unter dem angegebenen Lesezeichenpfad anzeigen können.

5. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

Registerkarte „Options“

Auf der Registerkarte **Options** können Sie die Optionen zum Navigieren in Windows- und UNIX/NFS-Netzwerken angeben. Dies beinhaltet auch die Möglichkeit, Ressourcen anzuzeigen und Ordnerlesezeichen zu erstellen. Diese Optionen werden zusammen mit den Dateiressourcenrichtlinien verwendet.

Angeben von allgemeinen Optionen zum Navigieren durch Dateien

So geben Sie allgemeine Optionen für die Dateinavigation an:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Rollenname* **> Web > Options**.

2. Geben Sie unter **Windows Network Files** die Optionen an, die für Benutzer aktiviert werden sollen:

   - **User can browse network file shares** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Windows-Dateifreigaben anzuzeigen und zu erstellen.

   - **User can add bookmarks** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Windows-Dateifreigaben anzuzeigen und zu erstellen.

3. Geben Sie unter **UNIX Network Files** die Optionen an, die für Benutzer aktiviert werden sollen:

   - **User can browse network file shares** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren UNIX-Dateifreigaben anzuzeigen und zu erstellen.

   - **User can add bookmarks** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren UNIX-Dateifreigaben anzuzeigen und zu erstellen.

   - **Allow automount shares** – Diese Option ermöglicht es Benutzern, auf Automount-Freigaben zuzugreifen, die auf einem NIS-Server angegeben sind.

4. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „Telnet/SSH“

Die Seite **Telnet/SSH** enthält die folgenden Registerkarten:

- „Registerkarte „Sessions““ auf Seite 296 – Auf dieser Registerkarte können Sie Lesezeichen für sichere Terminalsitzungen erstellen, die für dieser Rolle zugeordnete Benutzer auf der Willkommensseite angezeigt werden.
- „Registerkarte „Options““ auf Seite 297 – Auf dieser Registerkarte können Sie Benutzern das Erstellen eigener Telnet/SSH-Lesezeichen und das Aufrufen von Terminalsitzungen ermöglichen, und zudem können Sie das IVE so konfigurieren, dass Telnet/SSH-Ressourcenrichtlinien erstellt werden, die den Zugriff auf die in den Sitzungslesezeichen angegebenen Server gewähren.

Registerkarte „Sessions“

Auf der Registerkarte **Sessions** können Sie Lesezeichen für sichere Terminalsitzungen erstellen, die für dieser Rolle zugeordnete Benutzer auf der Willkommensseite angezeigt werden. In Lesezeichen für Terminalsitzungen sind Informationen zu Terminalsitzungen für Telnet- oder SSH-Sitzungen festgelegt, die von Benutzer gestartet werden können Diese Sitzungen gewähren Benutzern Zugriff auf eine Reihe von vernetzten Geräten, beispielsweise UNIX-Server, Netzwerkgeräte und andere Legacyanwendungen, die Terminalsitzungen verwenden. Das IVE unterstützt die SSH-Versionen V1 und V2 und verwendet die folgenden SSH-Versionen: OpenSSH_2.9.9p1, SSH protocols 1.5/2.0 und OpenSSL 0x0090607f.

Wenn Sie die Option für den sicheren Terminalzugriff (Telnet/SSH) aktivieren, den Benutzern jedoch nicht die Möglichkeit bieten, eigene Lesezeichen zu erstellen (siehe „Registerkarte „Options““ auf Seite 297), müssen Sie unbedingt Sitzungslesezeichen für die Benutzer konfigurieren. Andernfalls können Benutzer diese Funktion nicht verwenden.

Erstellen von Lesezeichen für sichere Terminalsitzungen

So erstellen Sie Lesezeichen für sichere Terminalsitzungen:

1. Wählen Sie in der Webkonsole die Optionen **Users** > **Roles** > *Rollenname* > **Telnet/SSH** > **Sessions**.
2. Klicken Sie auf **Add Session**. Die Seite **New Telnet/SSH Session** wird geladen.
3. Geben Sie bei Bedarf einen Lesezeichennamen und eine Beschreibung für die neue Telnet/SSH-Sitzung ein. Wenn Sie einen Namen und eine Beschreibung für ein Lesezeichen angeben, werden diese Informationen auf der Seite **Terminal Sessions** angezeigt.
4. Geben Sie ins Feld **Host** den Namen oder die IP-Adresse des Remotehosts für diese Sitzung ein.
5. Wählen Sie den **Session Type**, entweder **Telnet** oder **SSH Secure Shell,** und geben Sie geben Sie den Port an, falls dieser sich von der vorkonfigurierten Portzuordnung unterscheidet.

6. Geben Sie einen Benutzernamen ein, oder verwenden Sie die Variable <username> oder eine andere für IVE geeignete Sitzungsvariable.

7. Legen Sie unter **Font Size** durch Auswahl einer der folgenden Optionen die Schriftgröße fest:

   - **Fixed size of _ pixels** – Geben Sie eine Größe zwischen 8 und 36 Pixeln ein.

   - **Resize to fit window** – Ändert die Schriftgröße dynamisch beim Ändern der Fenstergröße. Diese Option erfordert Internet Explorer.

8. Wählen Sie in der Dropdownliste die Bildschirmgröße aus.

9. Geben Sie einen Wert für **Screen Buffer** ein.

10. Klicken Sie auf **Save Changes** oder **Save + New**.

HINWEIS: Erstellen Sie zusätzlich zu den Lesezeichen für sichere Terminalsitzungen eine Ressourcenrichtlinie, die Telnet/SSH-Sitzungen für die Rolle zulässt, oder aktivieren Sie auf der Registerkarte **Telnet/SSH > Options Auto-allow role Telnet/SSH sessions**, um den Zugriff auf die im Sitzungslesezeichen definierten Ressourcen automatisch zu genehmigen.

Registerkarte „Options“

Auf der Registerkarte **Options** können Sie es den Benutzern ermöglichen, eigene Telnet/SSH-Lesezeichen zu erstellen und Terminalsitzungen aufzurufen. Zudem können Sie das IVE so zu konfigurieren, dass Telnet/SSH-Ressourcenrichtlinien erstellt werden, die den Zugriff auf die in den Sitzungslesezeichen angegebenen Server gewähren.

Wenn Sie Benutzern das Navigieren zu einer Terminalsitzung ermöglichen, ist zu beachten, dass dies auf zweierlei Weise erfolgen kann:

- **Use the IVE homepage** – Die Benutzer können den gewünschten Server und den Port auf der IVE-Startseite in das Feld **Address** eingeben. Dabei sind folgende URL-Formate gültig:

  - Telnet://host:port

  - SSH://host:port

  Beispiel: Telnet://terminalserver.eigenefirma.com:3389

- **Use the Web browser’s address bar** – Die Benutzer können den gewünschten Server und Port (sowie Sitzungsparameter wie Schriftart und Fenstergröße) in der Adressleiste des Webbrowsers mithilfe des Standardwebprotokolls eingeben. Beispiel:

  https://iveserver/dana/term/newlaunchterm.cgi?protocol=telnet&host=termsrv.yourcompany.com&port=23&username=jdoe&fontsize=12&buffer=800&size=80x25

Angeben allgemeiner Optionen für Telnet/SSH

So geben Sie allgemeine Optionen für Telnet/SSH an:

1. Wählen Sie in der Webkonsole die Optionen **Users** > **Roles** > *Rollenname* > **Telnet/SSH** > **Options**.

2. Aktivieren Sie die Option **User can add sessions**, damit Benutzer eigene Sitzungslesezeichen definieren können und anhand der Syntax telnet:// und ssh:// sowie /dana/term/newlaunchterm.cgi zu einer Terminalsitzung navigieren können. Wenn Sie diese Option aktivieren, wird bei der nächsten Aktualisierung der IVE-Willkommensseite durch einen Benutzer die Schaltfläche **Add Terminal Session** auf der Seite **Terminal Sessions** angezeigt.

3. Aktivieren Sie die Option **Auto-allow role Telnet/SSH sessions**, damit durch das IVE automatisch der Zugriff auf die im Sitzungslesezeichen definierten Ressourcen gewährt wird (und keine Ressourcenrichtlinien erstellt werden müssen). Beachten Sie, dass dies nur für Rollenlesezeichen und nicht für Benutzerlesezeichen gilt.

4. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „Network Connect“

Auf der Registerkarte **Network Connect** können Sie Optionen für das Teilen von Tunneln, die automatische Deinstallation und die GINA-Funktion (Graphical Identification and Authentication) für eine Rolle festlegen. Weitere Informationen zu GINA finden Sie unter „Automatische Network Connect-Anmeldung mit „GINA““ auf Seite 98.

So legen Sie Network Connect-Optionen für das Teilen von Tunneln, den automatischen Start, die automatische Deinstallation und die GINA-Installation fest:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles >** *Rollenname* **> Network Connect**.

2. Wählen Sie unter **Split Tunneling Options** eine der folgenden Optionen aus:

   - **Disable Split Tunneling** – Der gesamte Netzwerkverkehr des Clients erfolgt über den Network Connect-Tunnel. Wenn durch Network Connect erfolgreich eine Verbindung mit dem IVE hergestellt wird, werden durch das IVE alle vordefinierten lokalen Subnetzrouten und von Host zu Host verlaufende Routen entfernt, die zur Tunnelteilung führen könnten. Wenn die lokale Routingtabelle während einer aktiven Network Connect-Sitzung geändert wird, wird die Sitzung vom IVE beendet.

   - **Allow access to local subnet** – Das IVE behält die lokale Subnetzroute auf dem Client bei, sodass der Zugriff auf lokale Ressourcen wie Drucker beibehalten wird. Die lokale Routingtabelle kann während der Network Connect-Sitzung geändert werden.

   - **Enable Split Tunneling** – Diese Option aktiviert die Teilung von Tunneln und erfordert, dass Sie gemäß den Anweisungen unter „Schreiben einer Network Connect-Ressourcenrichtlinie für Netzwerke mit geteilten Tunneln“ auf Seite 351 die Netzwerk-IP-Adresse/Netzmasken-Kombinationen angeben, für die das IVE Datenverkehr zwischen dem Remoteclient und dem Firmenintranet verarbeitet.

     Wenn geteilte Tunnel verwendet werden, ändert Network Connect Routen auf Clients, damit an das Firmenintranet gerichteter Verkehr an Network Connect und jeder weitere Verkehr über den lokalen physischen Adapter geleitet wird. Das IVE versucht, alle DNS-Anforderungen zunächst über den physischen Adapter aufzulösen, und leitet anschließend die fehlgeschlagenen Anforderungen an den Network Connect-Adapter weiter.

   - **Enable Split Tunneling with route change monitor** – Nach Beginn einer Network Connect-Sitzung führen Änderungen an der lokalen Routingtabelle zur Beendigung der Sitzung. Mit dieser Option wird der Zugriff auf lokale Ressourcen wie Drucker beibehalten.

3. Legen Sie unter **Auto Uninstall Options** fest, ob Network Connect sich selbst vom Remoteclient deinstalliert, wenn sich ein Benutzer von der Network Connect-Sitzung abmeldet.

4. Geben Sie unter **GINA Options** an, ob die GINA-Installation für eine Rolle aktiviert werden soll, und legen Sie durch Auswahl einer der folgenden Optionen das GINA-Anmeldeverhalten fest:

   - **Require NC to start when logging into Windows** – Nachdem GINA installiert wurde, startet diese Option bei jeder Anmeldung eines Windows-Benutzers automatisch die Network Connect-Anmeldefunktion.

   - **Allow user to decide whether to start NC when logging into Windows** – Nachdem GINA installiert wurde, ermöglicht diese Option dem Benutzer, bei jedem Windows-Start anzugeben, ob Network Connect gestartet werden soll.

5. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „New User“

Erstellen lokaler Benutzer

Wenn Sie als Typ Ihres Authentifizierungsservers „IVE Authentication“ auswählen, müssen Sie für diese Datenbank Datensätze für lokale Benutzer definieren. Lokale Benutzerdatensätze bestehen aus einem Benutzernamen, dem vollständigen Namen und dem Kennwort des Benutzers. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie schnell eine Gruppe von temporären Benutzern erstellen möchten.

So erstellen Sie lokale Benutzerdatensätze für die lokale IVE-Authentifizierung

1. Führen Sie in der Webkonsole einen der folgenden Vorgänge aus:
   - Wählen Sie **Signing In > AAA Servers** aus, klicken Sie auf die IVE-Datenbank, der Sie ein Benutzerkonto hinzufügen möchten, wählen Sie die Registerkarte **Users** aus, und klicken Sie dann auf **New**.
   - Wählen Sie **Users > New User** aus.
2. Geben Sie den Benutzernamen, den vollständigen Namen des Benutzers und ein Kennwort ein. Hinweis:
   - In Benutzernamen darf die Zeichenkombination „ ~ ~ “ nicht enthalten sein.
   - Wenn Sie den Benutzernamen eines Benutzers nach dem Erstellen seines Kontos ändern möchten, müssen Sie ein neues Konto erstellen.
3. (Nur auf der Seite **Users > New User**) Wählen Sie aus der Liste **Authenticate Using** die IVE-Datenbank aus, der Sie ein Benutzerkonto hinzufügen möchten.
4. Klicken Sie auf **Save Changes**. Der Benutzerdatensatz wird der IVE-Datenbank hinzugefügt.

Kapitel 10

Ressourcenrichtlinieneinstellungen

Auf der Webkonsole können Sie mithilfe der Einstellungen im Abschnitt **Resource Policies** individuelle Ressourcenrichtlinien erstellen und konfigurieren.

Inhalt

- „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305
- „Schreiben einer detaillierten Regel“ auf Seite 306
- „Konfigurieren der Seite „Web““ auf Seite 308
- „Konfigurieren der Seite „Files““ auf Seite 332
- „Konfigurieren der Seite „Telnet/SSH““ auf Seite 341
- „Konfigurieren der Seite „Network Connect““ auf Seite 344
- „Konfigurieren der Seite „Email Client““ auf Seite 354

Angeben von Ressourcen für eine Ressourcenrichtlinie

Für das IVE-Plattformmodul, das Ressourcenrichtlinien auswertet, müssen die in der Liste **Resources** einer Richtlinie aufgelisteten Ressourcen im kanonischen Format aufgeführt sein. Wenn ein Benutzer versucht, auf eine bestimmte Ressource zuzugreifen, vergleicht eine IVE-Appliance die angeforderte Ressource mit den in den entsprechenden Richtlinien angegebenen Ressourcen. Es beginnt dabei mit der ersten Richtlinie in der Richtlinienliste. Wenn das Modul eine angeforderte Ressource mit einer in der Liste **Resources** einer Richtlinie angegebenen Ressource abgleicht, wertet es weitere Richtlinieneinschränkungen aus und gibt die entsprechende Aktion an die Appliance zurück (es werden keine weiteren Richtlinien ausgewertet). Wenn keine Richtlinie zutrifft, wird die Standardaktion für die Richtlinie zurückgegeben.

Allgemeine Anmerkungen zu kanonischen Formaten

- Der Hostname und die IP-Adresse einer Ressource werden gleichzeitig an das Richtlinienmodul weitergegeben. Wenn ein Server in der Liste **Resources** einer Richtlinie als IP-Adresse angegeben ist, erfolgt die Auswertung anhand der IP-Adresse. Andernfalls versucht das Modul, die beiden Hostnamen abzugleichen. Es führt kein Reverse-DNS-Lookup zur Ermittlung der IP-Adresse durch.

- Wenn ein Hostname in der Liste **Resources** einer Richtlinie nicht vollständig qualifiziert ist, wenn z. B. „juniper“ anstelle von „intranet.juniper.net“ angegeben ist, führt das Modul die Auswertung anhand der vorliegenden Angaben durch. Der Hostname wird nicht weiter qualifiziert.

Angeben von Serverressourcen

Beachten Sie bei der Angabe von Serverressourcen für Network Connect-Ressourcenrichtlinien Folgendes.

Kanonisches Format: [Protokoll://]Host[:Ports]

Die drei Bestandteile sind:

- **Protokoll (optional)** – Mögliche Werte (Groß- oder Kleinschreibung wird nicht berücksichtigt):

  - tcp
  - udp
  - icmp

  Wenn kein Protokoll angegeben ist, werden alle drei Protokolle angenommen. Bei der Eingabe eines Protokolls muss das Trennzeichen „://“ eingegeben werden. Sonderzeichen sind nicht zulässig.

- **Host (erforderlich)** – Mögliche Werte:

  - **DNS-Hostname** – Beispiel: www.juniper.com

Sonderzeichen sind zulässig, einschließlich:

Tabelle 12: Sonderzeichen für DNS-Hostname

*****	Entspricht ALLEN Zeichen
%	Entspricht einem beliebigen Zeichen außer dem Punkt (.)
?	Entspricht genau einem Zeichen

Tabelle 13: Mögliche Werte für Port

*****	Entspricht ALLEN Ports, andere Sonderzeichen sind nicht zulässig.
Port[,Port]*	Eine durch Kommata getrennte Liste einzelner Ports. Gültige Portnummern sind [1-65535].
[Port 1]-[Port 2]	Ein Portbereich, von Port 1 bis Port 2 einschließlich.

Schreiben einer detaillierten Regel

Mit detaillierten Regeln kann die Ressourcenzugriffssteuerung flexibler gestaltet werden, sodass bestehende Ressourcen- oder Berechtigungsinformationen zum Angeben anderer Anforderungen für andere Benutzer verwendet können, auf die die Basisressourcenrichtlinie angewendet wird. Weitere Informationen finden Sie unter „Ausführliche Regeln für Ressourcenrichtlinien“ auf Seite 60.

So schreiben Sie eine detaillierte Regel für eine Ressourcenrichtlinie:

1. Geben Sie auf der Seite **New Policy** für eine Ressourcenrichtlinie die erforderlichen Ressourcen- und Rolleninformationen ein.

2. Wählen Sie im Bereich **Action** die Option **Use Detailed Rules** aus, und klicken Sie auf **Save Changes**.

3. Klicken Sie auf der Registerkarte **Detailed Rules** auf **New Rule**.

4. Führen Sie auf der Seite **Detailed Rule** Folgendes aus:

    a. Konfigurieren Sie im Bereich **Action** die Aktion, die ausgeführt werden soll, wenn die Benutzeranforderung einer Ressource in der Liste **Resource** entspricht (optional). Beachten Sie, dass die auf der Registerkarte **General** angegebene Aktion standardmäßig übertragen wird.

    b. Geben Sie im Bereich **Resources** eine der folgenden Optionen an (erforderlich):

        - Die vollständige oder einen Teil der Ressourcenliste, die auf der Registerkarte **General** angegeben ist.

        - Einen bestimmten Pfad oder eine bestimmte Datei auf den Servern, die auf der Registerkarte **General** angegeben sind. Gegebenenfalls können Platzhalter verwendet werden. Informationen zum Verwenden von Platzhaltern in einer **Resources**-Liste finden Sie in der Dokumentation der entsprechenden Ressourcenrichtlinie.

- Ein Dateityp, dem gegebenenfalls ein Pfad vorangestellt ist, oder geben Sie einfach **/*.Dateierweiterung* an, um Dateien mit der angegebenen Erweiterung innerhalb aller Pfade auf den Servern anzuzeigen, die auf der Registerkarte **General** angegeben sind.

c. Geben Sie im Abschnitt **Conditions** mindestens einen Ausdruck an, der für die Ausführung der Aktion ausgewertet wird (optional):

- Boolesche Ausdrücke: Schreiben Sie unter Verwendung von Systemvariablen mindestens einen booleschen Ausdruck mit den Operatoren NOT, OR oder AND. Eine Liste der in Ressourcenrichtlinien verfügbaren Variablen finden Sie unter „Systemvariablen und Beispiele“ auf Seite 401.

- Benutzerdefinierte Ausdrücke: Schreiben Sie unter Einhaltung der entsprechenden Syntax mindestens einen benutzerdefinierten Ausdruck. Informationen zur Syntax und zu Variablen finden Sie unter „Schreiben benutzerdefinierter Ausdrücke“ auf Seite 397. Beachten Sie, dass benutzerdefinierte Ausdrücke nur mit der erweiterten Lizenz verfügbar sind.

d. Klicken Sie auf **Save Changes**.

5. Ordnen Sie die Regeln auf der Registerkarte **Detailed Rules** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Sobald das IVE für die vom Benutzer angeforderte Ressource eine entsprechende Ressource in der Liste **Resource** für eine Regel findet, wird die angegebene Aktion durchgeführt und die Verarbeitung der Regeln (und weiterer Ressourcenrichtlinien) beendet.

Konfigurieren der Seite „Web“

Die Seite **Resource Policies > Web** enthält die folgenden Registerkarten:

- „Registerkarte „Access““ auf Seite 311 – Auf der Registerkarte **Access** können Sie eine Webressourcenrichtlinie schreiben, die steuert, auf welche Webressourcen Benutzer zugreifen können, um eine Verbindung mit dem Internet, Intranet oder Extranet herzustellen.
- „Registerkarten „Caching““ auf Seite 312 – Auf den **Caching**-Registerkarten können Sie Ressourcenrichtlinien für den Webzugriff erstellen und allgemeine Zwischenspeicherungsoptionen einstellen.
- „Registerkarten „Java““ auf Seite 316 – Auf den **Java**-Registerkarten können Sie Ressourcenrichtlinien erstellen, die die für Java-Applets verfügbaren Server und Ports definieren, und Sie können festlegen, wie das IVE Java-Applets neu schreibt.
- „Registerkarten „Rewriting““ auf Seite 320—Die **Rewriting**-Registerkarten dienen zum Erstellen von selektiven Ressourcenrichtlinien, Ressourcenrichtlinien für Durchgangsproxies und Ressourcenrichtlinien zum Umschreiben von ActiveX-Parametern.
- „Registerkarten „Web Proxy““ auf Seite 328 – Auf den **Web Proxy**-Registerkarten können Sie Ressourcenrichtlinien für Webproxies erstellen und Webproxyserver angeben.
- „Registerkarte „Compression““ auf Seite 330 – Die Registerkarte **Compression** dient zum Erstellen einer Ressourcenrichtlinie für die Webkomprimierung.
- „Registerkarte „Options““ auf Seite 331 – Auf der Registerkarte **Options** können Sie wie beschrieben Webressourcenoptionen festlegen.

Schreiben einer Webressourcenrichtlinie

Wenn Sie einer Rolle Zugriff auf das Web gewähren, müssen Sie Ressourcenrichtlinien erstellen, die angeben, auf welche Ressourcen ein Benutzer zugreifen darf, und ob das IVE den vom Benutzer angeforderten Inhalt neu schreiben muss. Zudem müssen Sie Angaben zur Zwischenspeicherung und zu Appletanforderungen machen. Für jede Webanforderung ermittelt das IVE die konfigurierten[1] Richtlinien für das Neuschreiben. Wenn der Benutzer eine Ressource anfordert, die nicht neu geschrieben werden darf („don’t rewrite“), weil sie entweder selektiv neu geschrieben werden soll oder aufgrund einer Ressourcenrichtlinie für Durchgangsproxy, leitet das IVE die Anforderung des Benutzers an die entsprechende Back-End-Ressource weiter. Andernfalls setzt das IVE die Auswertung der Ressourcenrichtlinien fort, die der Anforderung entsprechen, wie z. B. Java-Ressourcenrichtlinien bei der Anforderung eines Java-Applet. Wenn das IVE für eine Benutzeranforderung einer Ressource, die in der entsprechenden Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

1. Wenn Sie kein Neuschreiben von Ressourcenrichtlinien („Rewriting“) konfigurieren, setzt das IVE die Auswertung anhand der Richtlinien fort, die für die Anforderung des Benutzers gelten.

Beim Schreiben einer Webressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen** – Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Webrichtlinie müssen Sie wie in den folgenden Abschnitten beschrieben Webserver oder bestimmte URLs angeben.

- **Rollen** – Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.

- **Actions** – Jeder Typ von Ressourcenrichtlinie führt eine bestimmte Aktion aus: Zugriff auf eine Ressource gewähren bzw. verweigern oder eine Funktion, wie Neuschreiben von Inhalten, Neusignieren von Applets, Bereitstellen von Webdaten ausführen bzw. nicht ausführen. Sie können auch detaillierte Regeln schreiben, mit denen Sie weitere Bedingungen für eine Benutzeranforderung festlegen. Siehe „Schreiben einer detaillierten Regel“ auf Seite 306.

Für das IVE-Plattformmodul, das Ressourcenrichtlinien auswertet, müssen die in der Liste **Resources** einer Richtlinie aufgelisteten Ressourcen wie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305 beschrieben im kanonischen Format aufgeführt sein.

In diesem Abschnitt werden spezielle Aspekte behandelt, die beim Angeben einer Webressource im kanonischen Format beachtet werden müssen.

Kanonisches Format:

[Protokoll://]Host[:Ports][/Pfad]

Die vier Bestandteile sind:

- **Protokoll** (optional) – Mögliche Werte: http und https (Groß- oder Kleinschreibung wird nicht berücksichtigt)

  Wenn das Protokoll fehlt, werden sowohl http als auch https angenommen. Bei der Eingabe eines Protokolls muss das Trennzeichen „://“ eingegeben werden. Sonderzeichen sind nicht zulässig.

- **Host** (erforderlich) – Mögliche Werte:

  - **DNS-Hostname** – Beispiel: www.juniper.com

    Die zulässigen Sonderzeichen werden in der folgenden Tabelle beschrieben:

Tabelle 14: Sonderzeichen für DNS-Hostname

*	Entspricht ALLEN Zeichen
%	Entspricht einem beliebigen Zeichen außer dem Punkt (.)
?	Entspricht genau einem Zeichen

- **IP-Adresse/Netzmaske** – Die IP-Adresse muss in folgendem Format angegeben werden: a.b.c.d

  Die Netzmaske kann in einem der beiden folgenden Formate angegeben werden:

  - Präfix: Obere Bits
  - IP: a.b.c.d

  Beispiel: 10.11.149.2/24 oder 10.11.149.2/255.255.255.0

  Sonderzeichen sind nicht zulässig.

- **Ports** – Wenn Sie eine IP-Adresse/Netzmaske als Ressource angeben, müssen Sie einen Port festlegen. Bei einem DNS-Hostnamen ist der Port optional. Bei der Angabe eines Ports muss das Trennzeichen „:“ eingegeben werden. Beispiel: 10.11.149.2/255.255.255.0:*

Tabelle 15: Mögliche Werte für Port

*	Entspricht ALLEN Ports, andere Sonderzeichen sind nicht zulässig.
Port[,Port]*	Eine durch Kommata getrennte Liste einzelner Ports. Gültige Portnummern sind [1-65535].
[Port 1]-[Port 2]	Ein Portbereich, von Port 1 bis Port 2 einschließlich.

HINWEIS: Sie können Portlisten und Portbereiche mischen. Beispiel: 80,443,8080-8090

Wenn kein Port angegeben ist, wird der Standardport 80 für http und 443 für https zugewiesen.

- **Pfad** (optional) – Wenn kein Pfad angegeben ist, wird von einem Sternchen (*) ausgegangen, was bedeutet, dass ALLE Pfade zutreffen. Bei der Angabe eines Pfades muss das Trennzeichen „/“ eingegeben werden. Es werden keine weiteren Sonderzeichen unterstützt. Beispiel:
  - http://www.juniper.com:80/*
  - https://www.juniper.com:443/intranet/*
  - *.yahoo.com:80,443/*
  - %.danastreet.net:80/share/users/<Benutzername>/*

Registerkarte „Access“

Auf der Registerkarte **Access** können Sie eine Webressourcenrichtlinie schreiben, die steuert, auf welche Webressourcen Benutzer zugreifen können, um eine Verbindung mit dem Internet, Intranet oder Extranet herzustellen. Sie können den Zugriff auf Webressourcen nach URL oder IP-Bereich zulassen bzw. verweigern. Für URLs können Sie die Platzhalter „*“ und „?“ verwenden, um mehrere Hostnamen und Pfade anzugeben. Für mit dem Hostnamen angegebene Ressourcen können Sie außerdem HTTP, HTTPS oder beide Protokolle auswählen.

Schreiben einer Ressourcenrichtlinie für den Webzugriff

So schreiben Sie eine Ressourcenrichtlinie für den Webzugriff:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > Access** aus.

2. Klicken Sie auf der Seite **Web Access Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 331.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.

   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Allow access** – Hiermit gewähren Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen.

   - **Deny access** – Hiermit verweigern Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen.

   - **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Web Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 308.

Registerkarten „Caching“

Auf den **Caching**-Registerkarten können Sie Ressourcenrichtlinien für den Webzugriff erstellen und allgemeine Zwischenspeicherungsoptionen einstellen.

Registerkarte „Policies“

Auf der Registerkarte **Caching > Policies** können Sie eine Webressourcenrichtlinie schreiben, die steuert, welche Webinhalte auf einem Benutzercomputer zwischengespeichert werden. Die Zwischenspeicherung im Browser ist standardmäßig deaktiviert, so dass das IVE sämtliche Seiten, die für Remotebenutzer bereitgestellt werden, als nicht zwischenspeicherungsfähig markiert. Durch diese Einstellung wird verhindert, dass vertrauliche Seiten auf Remotecomputern verbleiben, nachdem ein Benutzer den Browser geschlossen hat. Diese Option kann jedoch auch zu einer Verlangsamung des Browsers führen, weil sie zum wiederholten Abrufen von Inhalten führt. Bei sehr langsamen Verbindungen können Probleme mit der Systemleistung auftreten. Alternativ können Sie eine Richtlinie angeben, die gestattet, dass einige Inhalte wie Bilder, die eine bestimmte Größenbeschränkung nicht überschreiten, zwischengespeichert werden können.

Dieser Abschnitt enthält die folgenden Informationen zu Zwischenspeicherungsrichtlinien:

- „Schreiben einer Ressourcenrichtlinie für die Webzwischenspeicherung“ auf Seite 312
- „Erstellen von OWA- und Lotus Notes-Ressourcenrichtlinien für die Zwischenspeicherung“ auf Seite 315

Schreiben einer Ressourcenrichtlinie für die Webzwischenspeicherung

So schreiben Sie eine Ressourcenrichtlinie für die Webzwischenspeicherung:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Caching > Policies** aus.

2. Klicken Sie auf der Seite **Web Caching Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 331.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.

   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Wählen Sie im Abschnitt **Action** eine der folgenden Optionen:

   - **Smart Caching (send headers appropriate for content and browser)** – Wählen Sie diese Option, damit das IVE basierend auf dem Webbrowser und Inhaltstyp des Benutzers einen cache-control:no-store-Header oder einen cache-control:no-cache-Header senden kann.

     Bei Verwendung dieser Option wird die Zuverlässigkeit von Medien- und Zip-Dateien erhöht, da die cache-control-Header des Quellservers entfernt werden. Mit der folgenden Logik wird z. B. nach „msie“ oder „windows-media-player“ in Benutzer-Agent-Headern gesucht, um die cache- oder cache-control:no-store-Antwortheader zu entfernen und die Dateien zwischenspeicherfähig zu machen:

     (wenn „content type“ das Element „audio/x-pn-realaudio“ enthält ODER
     wenn „content type“ mit „video/“ beginnt ODER
     wenn „content type“ mit „audio/“ beginnt ODER
     wenn „content type“ auf „application/octet-stream“ eingestellt ist und die Dateierweiterung mit „rm“ oder „ram“ beginnt
)

     Wenn das IVE im Benutzer-Agent-Header „msie“ oder „windows-media-player“ erkennt

     - und sich die Anforderung auf Flash-Dateien, XLS-, PPS- und PPT-Dateien bezieht,

     - und der „Content-Type“ application/, text/rtf, text/xml, model/ ist oder

     - wenn der Ursprungsserver einen „Content-Disposition“-Header sendet,

     sendet das IVE den cache-control:no-store-Header und entfernt den Cachesteuerungs-Header des Ursprungsservers.

In allen anderen Fällen fügt das IVE die Antwortheader pragma:no-cache oder cache-control:no-store hinzu.

HINWEIS: ICA-Dateien von Citrix und QuickPlace-Dateien werden anders behandelt. ICA-Dateien von Citrix sind immer zwischenspeicherungsfähig und erhalten auch den Header „cache-control-private“. QuickPlace-Dateien, die keiner festgelegten Regel (die Vorrang hat) entsprechen, erhalten die Header CCNS und „cache-control:private“.

Wenn Sie diese Option auswählen, die GZIP-Komprimierung aktivieren und mit Domino Web Access 6.5 über Internet Explorer auf eine angehängte Textdatei zugreifen, können Sie den Anhang nicht öffnen. Um Textanhänge öffnen zu können, müssen Sie entweder den Internet Explorer-Patch 323308 installieren oder die Option **Don't Cache (send "Cache Control: No Store")** aktivieren.

- **Don't Cache (send "Cache Control: No Store")** – Wählen Sie diese Option, um Anhänge an Internet Explorer zu senden, ohne sie auf der Festplatte zu speichern. (Der Browser schreibt die Dateien kurzfristig auf die Festplatte, entfernt sie aber sofort wieder, sobald die Datei im Browser geöffnet wird.) Wenn Sie diese Option auswählen, entfernt das IVE die Cachesteuerungs-Header des Ursprungsservers und fügt stattdessen einen Antwortheader vom Typ cache-control:no-store hinzu, falls die vom Browser gesendete User-Agent-Zeichenfolge „msie“ oder „windows-media-player“ enthält.

- **Don't Cache (send "Pragma: No Cache")** – Mit dieser Option können Sie verhindern, dass der Browser des Benutzers Dateien zwischenspeichert. Bei Auswahl dieser Option fügt das IVE den Antwortdateien den Standard-HTTP-Header pragma:no-cache und den Header cache-control:no-cache (CCNC-Header, HTTP 1.1) hinzu. Darüber hinaus leitet das IVE die Cacheheader des Ursprungsservers (beispielsweise age, date, etag, last-modified, expires) nicht weiter.

HINWEIS: Durch Senden der no-cache-Header für viele Typen von Anhängen (PDF, PPT, Streaming-Dateien) wird Internet Explorer gezwungen, diese Dokumente nicht zu bearbeiten, da der Browser diese Dokumente hierzu zeitweilig in den Cache schreiben muss.

- **Cache (do not add/modify caching headers)** – Das IVE fügt die Antwortheader pragma:no-cache oder cache-control:no-store nicht hinzu und leitet die Cacheheader des Ursprungsservers weiter.

- **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Web Caching Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 308.

Erstellen von OWA- und Lotus Notes-Ressourcenrichtlinien für die Zwischenspeicherung

Die folgende Tabelle enthält Beispiele für einige der Inhaltstypen, die das IVE mit den Anwendungen OWA und iNotes unterstützt. Darüber hinaus zeigt die Tabelle die Cachesteuerungsdirektiven, die Sie implementieren müssen, um das Öffnen und Speichern der angegebenen Inhaltstypen zu unterstützen.

Aus Leistungsgründen empfehlen wir die Erstellung von Zwischenspeicherungsrichtlinien für den gesamten Inhalt des iNotes-Verzeichnisses.

Tabelle 16: OWA-Ressourcenrichtlinien für Zwischenspeicherung

Anhangstyp	Öffnen des Anhangs:	Speichern des Anhangs:
zip	Smart Caching	Smart Caching
ppt	Smart Caching	Smart Caching
doc	Smart Caching	Smart Caching
xls	Smart Caching	Smart Caching
pdf	Smart Caching	Smart Caching
txt	Smart Caching	Cache control: No store
html	Smart Caching	Cache control: No store

Tabelle 17: iNotes-Ressourcenrichtlinien für Zwischenspeicherung

Anhangstyp	Öffnen des Anhangs:	Speichern des Anhangs:
zip	Cache control: No store	Cache control: No store
ppt	Cache control: No store	Cache control: No store
doc	Smart Caching	Smart Caching
xls	Cache control: No store	Cache control: No store
pdf	Cache control: No store	Cache control: No store
txt	Cache control: No store	Cache control: No store
html	Cache control: No store	Cache control: No store
andere Dateitypen	Cache control: No store	Cache control: No store

Registerkarte „Options“

Auf der Registerkarte **Caching > Options** können Sie die maximale Größe einer Bilddatei angeben, die auf einem Client zwischengespeichert werden kann. Wenn der „content-type“-Header des Ursprungsservers mit „image/“ beginnt und der „content-length“-Header eine Größe angibt, die kleiner ist als die für diese Option konfigurierte maximale Größe, leitet das IVE die Cacheheader des Ursprungsservers weiter. Andernfalls behandelt das IVE die Anforderung wie bei deaktivierter Zwischenspeicherung.

Angeben von allgemeinen Cacheoptionen

So geben Sie Cacheoptionen an:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Caching > Options** aus.
2. Geben Sie auf der Seite **Caching Options** eine maximal zulässige Bildgröße in das Feld **Clients should cache all images less than** ein.
3. Klicken Sie auf **Save Changes**.

Registerkarten „Java“

Auf den **Java**-Registerkarten können Sie Ressourcenrichtlinien erstellen, die die für Java-Applets verfügbaren Server und Ports definieren, und Sie können festlegen, wie das IVE Java-Applets neu schreibt. Die Registerkarten **Java** können auch verwendet werden, um Java-Applets in das IVE zu laden.

Access Control

Auf der Registerkarte **Java > Access Control** können Sie eine Webressourcenrichtlinie schreiben, die steuert, mit welchen Servern und Ports Java-Applets eine Verbindung herstellen können.

Schreiben einer Ressourcenrichtlinie für die Java-Zugriffssteuerung

So schreiben Sie eine Ressourcenrichtlinie für die Java-Zugriffssteuerung:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Java > Access Control** aus.
2. Klicken Sie auf der Seite **Java Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   a. Eine Bezeichnung für diese Richtlinie.
   b. Eine Beschreibung der Richtlinie (optional).
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 331.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Allow socket access** – Erlaubt, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Deny socket access** – Verhindert, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Java Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 308.

Registerkarte „Code Signing“

Auf der Registerkarte **Java > Code Signing** können Sie eine Webressourcenrichtlinie schreiben, die angibt, wie das IVE Java-Applets neu schreibt. Wenn das IVE ein signiertes Java-Applet vermittelt, signiert es das Applet standardmäßig mit einem eigenen Zertifikat neu, das nicht mit einem Standardstammzertifikat verkettet ist. Wenn ein Benutzer ein Applet anfordert, das Aufgaben mit einem hohen Risikopotential durchführt, z. B. Zugreifen auf Netzwerkserver, wird im Browser des Benutzers in einer Sicherheitswarnung angezeigt, dass der Stamm nicht vertrauenswürdig ist. Um die Anzeige dieser Warnung zu vermeiden, können Sie ein Codesignaturzertifikat importieren, mit dem das IVE zu vermittelnde Applets neu signiert. Weitere Informationen zu Codesignaturzertifikaten finden Sie unter „Codesignaturzertifikate“ auf Seite 72.

Beim Konfigurieren der Registerkarte **Java > Code Signing** geben Sie die Server, deren Applets Sie vertrauen, ins Feld **Resources** ein. Sie können die IP-Adresse oder den Domänennamen eines Servers eingeben. Das IVE signiert nur Applets neu, die von vertrauenswürdigen Servern stammen. Wenn ein Benutzer ein Applet anfordert, das von einem nicht in der Liste aufgeführten Server stammt, verwendet das IVE nicht die importierten Produktionszertifikate zum Signieren des Applets. Dies bedeutet, dass dem Benutzer im Browser eine Sicherheitswarnung angezeigt wird. Für Benutzer der Sun JVM überprüft das IVE außerdem, ob die Stammzertifizierungsstelle des ursprünglichen Appletzertifikats in der Liste vertrauenswürdiger Stammzertifizierungsstellen aufgeführt ist.

Schreiben einer Ressourcenrichtlinie für die Java-Codesignatur

So schreiben Sie eine Ressourcenrichtlinie für die Java-Codesignatur:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Java > Access Control** aus.

2. Klicken Sie auf der Seite **Java Signing Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 331.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.

   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Resign applets using applet certificate** – Erlaubt, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.

- **Resign applets using default certificate** – Verhindert, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.

- **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Java Signing Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 308.

Applets

Über die Registerkarte **Java > Applets** können Sie wie unter „Hochladen eines Java-Applets - Übersicht“ auf Seite 111 beschrieben Applets in das IVE laden.

HINWEIS: Maximal können Java-Applets mit einer Größe von insgesamt 100 MB in das IVE geladen werden. Das IVE zeigt die Größe jedes in das IVE geladenen Applets auf der Seite **Java Applets** an, so dass Sie bei Bedarf Applets löschen können.

Hochladen eines Java-Applets in das IVE

So laden Sie ein Java-Applet in das IVE hoch:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Java > Applets** aus.

2. Klicken Sie auf **New Applet**.

3. Geben Sie auf der Seite **New Java Applet** Folgendes ein:

   a. Eine Bezeichnung für dieses Java-Applet. (Wenn Sie einem Weblesezeichen mehrere Applets hinzufügen möchten, sollten Sie für alle Applets den gleichen Namen verwenden). Anschließend müssen Sie einfach diesen einen Namen auswählen, wenn Sie Ihre HTML-Datei über die Seite **Users > Roles >** *[Rolle]* **> Web > Bookmarks** generieren.)

   b. Eine Beschreibung des Applet (optional).

4. Wählen Sie im Abschnitt **Upload Applet** das Applet aus, das Sie in das IVE laden möchten. Applets mit den folgenden Erweiterungen können hochgeladen werden: .jar, .cab, .zip und .class.

5. Aktivieren Sie das Kontrollkästchen **Trusted Applet**, wenn Sie das Applet mit dem auf dem IVE installierten Codesignaturzertifikat neu signieren möchten (siehe „Signieren von hochgeladenen Java-Applets“ auf Seite 112).

HINWEIS: Das IVE deaktiviert diese Option, wenn Sie kein Appletzertifikat über die Seite **System > Configuration > Certificates > Code-Signing Certificates** in das IVE importieren.

6. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

7. Wenn der folgende Vertrag angezeigt wird, lesen Sie ihn, und klicken Sie auf **OK**, wenn Sie den Bedingungen zustimmen:

   You are about to load third party software onto the Juniper product. Before you do, you must read and agree to the following terms on behalf of yourself (as the purchaser of the equipment) or the organization that purchased the Juniper product, as applicable.

   By loading the third party software onto the Juniper product, you are responsible for obtaining all rights necessary for using, copying, and/or distributing such software in or with the Juniper product. Juniper is not responsible for any liability arising from use of such third party software and will not provide support for such software. The use of third party software may interfere with the proper operation of the Juniper product and/or Juniper software, and may void any warranty for the Juniper product and/or software.

   Click on the “OK” button if you agree and wish to continue.

8. Lesen Sie die Details im Dialogfeld **Upload Status**, und klicken Sie anschließend auf **OK**.

9. Erstellen Sie wie unter „Angeben von allgemeinen Webbrowsingoptionen“ auf Seite 288 beschrieben ein entsprechendes Weblesezeichen auf der Seite **Users > Roles >** *[Rolle]* **> Web > Bookmarks**.

Registerkarten „Rewriting“

Auf den **Rewriting**-Registerkarten können Sie Ressourcenrichtlinien für selektives Neuschreiben, Durchgangsproxies und das Neuschreiben von ActiveX-Parametern erstellen. Zudem können Sie Filter für das Neuschreiben hinzufügen, wenn Sie vom Juniper Networks-Support dazu aufgefordert werden.

Registerkarte „Selective Rewriting“

Auf der Registerkarte **Rewriting > Selective Rewriting** können Sie eine Webressourcenrichtlinie schreiben, die es Ihnen ermöglicht, eine Liste von Hosts festzulegen, für die das IVE Inhalt und Ausnahmen von der Liste vermittelt. Standardmäßig vermittelt das IVE alle Benutzeranforderungen für Webhosts, sofern Sie nicht die Anforderungsverarbeitung für bestimmte Hosts anhand eines anderen Verfahrens konfiguriert haben, z. B. Secure Application Manager.

Erstellen Sie eine Richtlinie für das selektive Neuschreiben, wenn das IVE den Datenverkehr von Websites vermitteln soll, die sich außerhalb des Firmennetzwerks befinden, z. B. yahoo.com, oder wenn das IVE keinen Datenverkehr für Client-/Serveranwendungen vermitteln soll, die Sie als Webressourcen bereitgestellt haben, z. B. Microsoft OWA (Outlook Web Access).

Schreiben einer Ressourcenrichtlinie für selektives Neuschreiben

So schreiben Sie eine Ressourcenrichtlinie für selektives Neuschreiben:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Rewriting > Selective Rewriting** aus.

2. Klicken Sie auf der Seite **Web Rewriting Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 331.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.

   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Rewrite content** – Das IVE vermittelt alle Webinhalte von den in der Liste **Resources** angegebenen Ressourcen. Neue IVE-Appliances werden mit einer anfänglichen Richtlinie für das Neuschreiben geliefert, die den gesamten Inhalt für alle Rollen neu schreibt.

- **Don't rewrite content** – Das IVE vermittelt keine Webinhalte von den in der Liste **Resources** angegebenen Ressourcen. Die ist die Standardoption für alle von Ihnen erstellten Ressourcenrichtlinien für das Neuschreiben. Bei Auswahl dieser Option können Sie festlegen, dass das IVE die nicht neu geschriebenen Seiten in einem neuen Fenster öffnet. Verwenden Sie dazu die Option unter „Registerkarte „Options"" auf Seite 331.

- **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Web Rewriting Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie" auf Seite 308.

Registkerarte „Pass-through Proxy"

Auf der Registerkarte **Rewriting > Pass-through Proxy** können Sie eine Webressourcenrichtlinie schreiben, die Webanwendungen angibt, für die das IVE nur minimale Vermittlung übernimmt. Zum Erstellen einer Ressourcenrichtlinie für Durchgangsproxys müssen Sie zwei Angaben machen:

- Die Webanwendungen, die über den Durchgangsproxy vermittelt werden.

- Die Art der Überwachung von Clientanforderungen an die Anwendungsserver durch das IVE.

Weitere Informationen zu dieser Funktion finden Sie unter „Durchgangsproxy – Übersicht" auf Seite 117.

Schreiben einer Ressourcenrichtlinie für Durchgangsproxys

So schreiben Sie eine Ressourcenrichtlinie für Durchgangsproxys:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Rewriting > Pass-through Proxy** aus.

2. Klicken Sie auf der Seite **Pass-through Proxy Policies** auf **New Application**.

3. Geben Sie auf der Seite **New Pass-through Application** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

4. Geben Sie im Feld **URL** den Hostnamen des Anwendungsservers und den Port für den internen Zugriff auf die Anwendung an. Sie können in dieses Feld keinen Pfad eingeben.

5. Wählen Sie aus, wie die Durchgangsproxyfunktion aktiviert werden soll:

   - **Use virtual hostname** – Wenn Sie diese Option auswählen, müssen Sie einen Hostnamenalias für den Anwendungsserver angeben. Wenn das IVE eine Clientanforderung für den Hostnamenalias des Anwendungsservers empfängt, leitet es die Anforderung an den angegebenen Anwendungsserverport im Feld **URL** weiter.

HINWEIS: Wenn Sie diese Option auswählen, müssen Sie auf der Registerkarte **System > Network > Internal Port** im Abschnitt **Network Identity** auch den IVE-Namen und den Hostnamen definieren.

   - **Use IVE port** – Bei Auswahl dieser Optionen müssen Sie einen eindeutigen IVE-Port zwischen 11000-11099 angeben. Das IVE überwacht den angegebenen IVE-Port und leitet alle Clientanforderungen an den Anwendungsserver an den Anwendungsserverport im Feld **URL** weiter.

6. Geben Sie im Bereich **Action** die Methode an, die das IVE zum Vermitteln des Datenverkehrs verwenden soll:

   - **Rewrite XML**
   - **Rewrite external links**
   - **Block cookies from being sent to the browser**
   - **Host-Header forwarding**

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Pass-through Proxy Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Anwendung, die von einem Benutzer angefordert wurde, zu einer in der Liste **Resource** angegebenen Anwendung für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

9. Wenn Sie Folgendes auswählen:

   - **Use virtual hostname**, müssen Sie außerdem Folgendes durchführen:

     i. Hinzufügen einen Eintrags für jeden Hostnamenalias eines Anwendungsservers im externen DNS, der für das IVE aufgelöst wird.

     ii. Hochladen eines Serverzertifikats mit Platzhaltern in das IVE (empfohlen).

- **Use IVE port**, müssen Sie Datenverkehr für den IVE-Port öffnen, den Sie für den Anwendungsserver in der Firmenfirewall angegeben haben.

HINWEIS: Wenn die Anwendung mehrere Ports überwacht, konfigurieren Sie jeden Anwendungsport als separaten Durchgangsproxyeintrag mit einem separaten IVE-Port. Wenn Sie über verschiedene Hostnamen oder IP-Adressen auf den Server zugreifen möchten, konfigurieren Sie jede dieser Optionen einzeln. In diesem Fall können Sie denselben IVE-Port verwenden.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 308.

Registerkarte „ActiveX Parameter Rewriting“

Wenn das IVE eine Webseite neu schreibt, werden dabei die in der Seite eingebetteten ActiveX-Steuerelemente nicht neu geschrieben. Mit Ressourcenrichtlinien können Sie jedoch festlegen, dass das IVE die URL- und Hostnamenparameter neu schreibt, die von der Webseite an die ActiveX-Steuerelemente weitergeleitet werden. Sie benötigen folgende Informationen, um diese Ressourcenrichtlinien zu konfigurieren:

- **Klassen-ID** – Ein ActiveX-Steuerelement wird auf Webseiten in der Regel mithilfe einer Klassen-ID eingebettet. Eine Klassen-ID ist eine eindeutige konstante Zeichenfolge, die das ActiveX-Steuerelement eindeutig identifiziert.

  Mit Internet Explorer 6 können Sie feststellen, welche Klassen-ID für ein ActiveX-Objekt verwendet wird: Wählen Sie **Extras > Internetoptionen**, klicken Sie auf **Einstellungen** und dann auf **Objekte anzeigen**. Wählen Sie das ActiveX-Objekt aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften**. Die ID des ActiveX-Objekts wird hervorgehoben.

- **Sprache** – Für Webseiten muss statischer oder dynamischer HTML-Code verwendet werden (d. h. Javascript), um ein Active X-Steuerelement einzubetten. Bei Verwendung von statischem HTML-Code kann das IVE die angegebenen ActiveX-Parameter auf dem IVE selbst neu schreiben bei gleichzeitiger Vermittlung von Datenverkehr, da alle erforderlichen Informationen zwischen dem Browser des Benutzers und dem Webserver der Anwendung geleitet werden. Wird auf einer Webseite jedoch dynamischer HTML-Code zum Einbetten eines ActiveX-Steuerelements verwendet, fordert die Seite häufig Informationen vom Client an und generiert dann den HTML-Code, um das ActiveX-Steuerelement einzubetten. Deshalb muss das IVE im Browser des Benutzers Skripts ausführen, um die erforderlichen Informationen für das Neuschreiben der angegebenen ActiveX-Parameter zu erhalten.

- **Parametertyp** – Wenn Sie das IVE zum Neuschreiben eines Parameters konfigurieren, müssen Sie angeben, ob es sich bei dem Parameter um einen URL oder einen Hostnamen handelt. Das IVE unterstützt keine anderen Parametertypen.

- **Parametername** – Geben Sie den Namen des Parameters an, der vom IVE Neu geschrieben werden soll. Sie finden die Parameter durch Suchen nach dem Param-Tag in einem Objekt-Tag. Sie können z. B. einen auf einer Seite eingebetteten Flash-Film mit folgendem Code finden:

```
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" > <param
name="movie" value="mymovie.swf" />

<param name="quality" value="high" />

</object>
```

Geben Sie beim Konfigurieren der entsprechenden Ressourcenrichtlinie ins Feld **Parameter name** movie ein, da movie auf den URL verweist, der umgeschrieben werden muss. Seiten enthalten häufig mehrere Param-Tags, jedoch müssen nicht alle umgeschrieben werden. In diesem Beispiel muss der Parameter quality nicht umgeschrieben werden.

Schreiben Sie eine Ressourcenrichtlinie zum Umschreiben von ActiveX-Parametern

So Schreiben Sie eine Ressourcenrichtlinie zum Umschreiben von ActiveX-Parametern:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Rewriting > ActiveX Parameter Rewriting**.
2. Klicken Sie auf der Seite **ActiveX Parameter Rewriting Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   a. Die Klassen-ID des ActiveX-Steuerelements, das mit der Richtlinie gesteuert werden soll.
   b. Eine Beschreibung der Richtlinie (optional).
4. Geben Sie im Abschnitt **Parameters** die ActiveX-Parameter an, die Sie mit der Richtlinie und den entsprechenden Aktionen steuern möchten. Mögliche Aktionen sind:
   - **Rewrite URL and response (Static HTML only)** – Das IVE schreibt den angegebenen URL-Parameter im IVE um. Das IVE schreibt auch die Antworten vom Webserver um, der den URL anfordert. Wählen Sie diese Option, wenn die Webseite das ActiveX-Steuerelement nur mit statischem HTML einbettet.
   - **Rewrite URL and response (Static and dynamic HTML)** – Zusätzlich zum Neuschreiben auf dem IVE schreibt das IVE den angegebenen URL auf dem Client neu. Das IVE schreibt auch die Antworten vom Webserver um, der den URL anfordert. Wählen Sie diese Option, wenn die Webseite das ActiveX-Steuerelement mittels dynamischem HTML einbettet.
   - **Rewrite URL (Static HTML only)** – Das IVE schreibt den angegebenen URL-Parameter im IVE um. Wählen Sie diese Option, wenn die Webseite das ActiveX-Steuerelement nur mit statischem HTML einbettet.
   - **Rewrite URL (Static and dynamic HTML)** – Zusätzlich zum Neuschreiben auf dem IVE schreibt das IVE den angegebenen URL auf dem Client neu. Wählen Sie diese Option, wenn die Webseite das ActiveX-Steuerelement mittels dynamischem HTML einbettet.

- **Rewrite hostname (Static HTML only)** – Das IVE schreibt den angegebenen Hostnamenparameter im IVE um. Wählen Sie diese Option, wenn die Webseite das ActiveX-Steuerelement nur mit statischem HTML einbettet.
- **Rewrite hostname (Static and dynamic HTML)** – Zusätzlich zum Neuschreiben auf dem IVE schreibt das IVE den angegebenen Hostnamen auf dem Client neu. Wählen Sie diese Option, wenn die Webseite das ActiveX-Steuerelement mittels dynamischem HTML einbettet.
- **Do not rewrite** – Das IVE schreibt keine Parameter der ActiveX-Komponente um.

5. Klicken Sie auf **Save Changes**.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 308.

Wiederherstellen der ActiveX-Standardressourcenparameter des IVE

Das IVE beinhaltet mehrere vordefinierte Ressourcenrichtlinien zum Umschreiben der Parameter häufig verwendeter ActiveX-Objekte. Wenn Sie gelöschte Ressourcen wieder herstellen möchten, verwenden Sie hierzu die folgende Tabelle als Richtlinie.

Tabelle 18: Vordefinierte Ressourcenrichtlinien

Beschreibung	Klassen-ID	Parameter	Aktion
Citrix NFuse xginen_EmbeddedApp object	238f6f83-b8b4-11cf-8771-00a024541ee3	ICAFile	Rewrite URL and response (Static HTML only)
OrgPlus OrgViewer	DCB98BE9-88EE-4AD0-9790-2B169E8D5BBB	URL	Rewrite URL and response (Static HTML only)
Quickplace	05D96F71-87C6-11D3-9BE4-00902742D6E0	GeneralURL	Rewrite URL and response (Static and dynamic HTML)
		General_ServerName	Rewrite host name (Static and dynamic HTML)
iNotes Discussion	5BDBA960-6534-11D3-97C7-00500422B550	FullURL	Rewrite URL and response (Static and dynamic HTML)
B20D9D6A-0DEC-4d76-9BEF-175896006B4A	B20D9D6A-0DEC-4d76-9BEF-175896006B4A	ServerURL	Rewrite URL and response (Static HTML only)
		Error URL	Rewrite URL and response (Static HTML only)
Citrix NFuse Elite	2E687AA8-B276-4910-BBFB-4E412F685379	ServerURL	Rewrite URL and response (Static HTML only)
WebPhotos LEAD	00120000-B1BA-11CE-ABC6-F5B2E79D9E3F	BitmapDataPath	Rewrite URL and response (Static and dynamic HTML)
Shockwave Flash	D27CDB6E-AE6D-11cf-96B8-444553540000	Src	Rewrite URL and response (Static and dynamic HTML)
		Movie	Rewrite URL and response (Static and dynamic HTML)

Tabelle 18: Vordefinierte Ressourcenrichtlinien (Fortsetzung)

Beschreibung	Klassen-ID	Parameter	Aktion
iNotes Blue	3BFFE033-BF43-11d5-A271-00A024A51325	General_URL	Rewrite URL and response (Static and dynamic HTML)
		General_ServerName	Rewrite host name (Static and dynamic HTML)
Tabular Data Control	333C7BC4-460F-11D0-BC04-0080C7055A83	DataURL	Rewrite URL (Static HTML only)
Windows Media Player	6BF52A52-394A-11D3-B153-00C04F79FAA6	URL	Rewrite URL and response (Static HTML only)
FlowPartPlace	4A266B8B-2BB9-47db-9B0E-6226AF6E46FC	URL	Rewrite URL and response (Static HTML only)
HTML-Hilfe	adb880a6-d8ff-11cf-9377-00aa003b7a11	Item1	Rewrite URL and response (Static and dynamic HTML)
MS Media Player	22d6f312-b0f6-11d0-94ab-0080c74c7e95	FileName	Rewrite URL and response (Static HTML only)
CSV-Dateihandler	333c7bc4-460f-11d0-bc04-0080c7055a83	DataURL	Rewrite URL and response (Static HTML only)
Spezielles ActiveX-Steuerelement für Microsoft OWA	D801B381-B81D-47a7-8EC4-EFC111666AC0	mailboxUrl	Rewrite URL and response (Static HTML only)
FlowPartPlace1	639325C9-76C7-4d6c-9B4A-523BAA5B30A8	Url	Rewrite URL and response (Static HTML only)
scriptx-Drucksteuerelement	5445be81-b796-11d2-b931-002018654e2e	Pfad	Rewrite URL and response (Static HTML only)
94F40343-2CFD-42A1-A774-4E7E48217AD4	94F40343-2CFD-42A1-A774-4E7E48217AD4	HomeViewURL	Rewrite URL and response (Static HTML only)
Microsoft License Manager	5220cb21-c88d-11cf-b347-00aa00a28331	LPKPath	Rewrite URL and response (Static HTML only)
Domino 7 beta 2 UploadControl	E008A543-CEFB-4559-912F-C27C2B89F13B	General_URL	Rewrite URL and response (Static and dynamic HTML)
		General_ServerName	Rewrite host name (Static and dynamic HTML)
iNotes	1E2941E3-8E63-11D4-9D5A-00902742D6E0	General_URL	Rewrite URL and response (Static and dynamic HTML)
		General_ServerName	Rewrite host name (Static and dynamic HTML)
ActiveCGM	F5D98C43-DB16-11CF-8ECA-0000C0FD59C7	FileName	Rewrite URL and response (Static HTML only)
00130000-B1BA-11CE-ABC6-F5B2E79D9E3F	00130000-B1BA-11CE-ABC6-F5B2E79D9E3F	BitmapDataPath	Rewrite URL and response (Static and dynamic HTML)

Registerkarte „Rewriting Filters“

Verwenden Sie diese Registerkarte nur, wenn Sie vom Juniper Networks-Supportteam dazu aufgefordert werden.

Registerkarten „Web Proxy“

– Auf den **Web Proxy**-Registerkarten können Sie Ressourcenrichtlinien für Webproxies erstellen und Webproxyserver angeben. Das IVE vermittelt Proxies in beiden Richtungen.

Registerkarte „Policies“

Auf den **Web Proxy**-Registerkarten können Sie Ressourcenrichtlinien für Webproxies erstellen, in denen Sie die von den Proxies zu schützenden Webserver angeben.

Schreiben einer Ressourcenrichtlinie für Webproxys

So schreiben Sie eine Ressourcenrichtlinie für Webproxys:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Web Proxy > Policies**.
2. Klicken Sie auf der Seite **Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   a. Eine Bezeichnung für diese Richtlinie.
   b. Eine Beschreibung der Richtlinie (optional).
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 331.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Access web resources directly** – Das IVE vermittelt die Anforderung des Benutzers an einen Back-End-Server und die Antwort des Servers an den Benutzer. Dies gilt für Anforderungen an eine in der Liste **Resources** angegebene Ressource.

   - **Access web resources through a web proxy** – Wählen Sie in der Dropdownliste einen Webproxyserver aus, den Sie auf der Registerkarte **Resource Policies > Web > Web Proxy > Servers** definiert haben. Informationen zum Definieren von Webproxyservern finden Sie unter „Registerkarte „Server““ auf Seite 329.

   - **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Web Proxy Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 308.

Registerkarte „Server“

Sie können alle vom IVE durchgeführten Webanforderungen an einen Webproxy leiten, statt mit dem IVE direkt eine Verbindung mit den Webservern herzustellen. Diese Funktion bietet sich an, wenn Ihre Richtlinien für die Netzwerksicherheit diese Konfiguration erfordern oder wenn Sie zur Leistungssteigerung einen Webproxy mit Zwischenspeicherung verwenden möchten.

HINWEIS: Derzeit wird die Authentifizierung über Webproxys vom IVE nicht unterstützt. Wenn Sie die Webproxyfunktion des IVE verwenden möchten, müssen Sie Ihren Webproxy so konfigurieren, dass nicht authentifizierte Benutzer akzeptiert werden.

Angeben von Webproxyservern

Auf der Registerkarte **Web Proxy** können Sie Server für Ressourcenrichtlinien für Webproxys angeben.

So geben Sie Webproxyserver an:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Web Proxy > Servers**.

2. Geben Sie unter **Web Proxy Servers** den Namen oder die IP-Adresse des Webproxyservers sowie die Portnummer ein, an der der Proxyserver Daten abfragt, und klicken Sie dann auf **Add**.

3. Wiederholen Sie diesen Schritt, um weitere Webproxyserver anzugeben.

Registerkarte „Compression“

Geben Sie auf der Registerkarte **Compression** an, welche Art von Webdaten das IVE komprimieren soll, wenn Sie auf der Seite **Maintenance > System > Options** die GZIP-Komprimierung aktivieren.

HINWEIS: Das IVE ist mit einer Webkomprimierungsrichtlinie (*:*/*) zur Komprimierung aller entsprechenden Webdaten vorkonfiguriert. Sie können diese Richtlinie über die Seiten **Resource Policies > Web > Compression** der Webkonsole aktivieren.

Schreiben einer Webkomprimierungsrichtlinie

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > Compression**.

2. Klicken Sie auf der Seite **Web Compression Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

4. Geben Sie im Bereich **Resources** die URLs an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 331.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.

   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Compress** – Das IVE komprimiert die unterstützten Inhaltstypen der angegebenen Ressource.

- **Do not compress** – Das IVE komprimiert die unterstützten Inhaltstypen der angegebenen Ressource nicht.
- **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

Registerkarte „Options“

Über die Registerkarte **Options** können Sie Webressourcenoptionen festlegen, die auf Ihre Webressourcenrichtlinien anwendbar sind. Folgende Optionen stehen zur Verfügung:

- **IP based matching for Hostname based policy resources** – Das IVE sucht nach IP-Adressen, die den in einer Webressourcenrichtlinie angegebenen Hostnamen entsprechen. Wenn ein Benutzer versucht, auf einen Server zuzugreifen, indem er eine IP-Adresse anstelle des Hostnamens angibt, vergleicht das IVE die IP mit einer zwischengespeicherten Liste von IP-Adressen, um festzustellen, ob ein Hostname mit einer IP übereinstimmt. Wenn eine Übereinstimmung vorliegt, akzeptiert das IVE diese als eine Richtlinienübereinstimmung und führt die für die Ressourcenrichtlinie angegebene Aktion durch.

HINWEIS: Diese Option wird nicht auf Hostnamen angewendet, die Platzhalter und Parameter enthalten.

- **Case sensitive matching for the Path and Query string components in Web resources** – Benutzer müssen für Ressourcen URLs unter Berücksichtigung der Groß- und Kleinschreibung eingeben. Verwenden Sie diese Option beispielsweise beim Übergeben des Benutzernamens oder des Kennwortes in einem URL.

Wenn Sie eine Webressourcenrichtlinie aktivieren, kompiliert das IVE eine Liste von Hostnamen, die im Feld **Resources** jeder Webressourcenrichtlinie angegeben wird. Das IVE wendet die aktivierten Optionen dann auf diese umfassende Liste von Hostnamen an.

Angeben von Webressourcenoptionen

So geben Sie eine Webressourcenoption an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > Options**.
2. Wählen Sie Folgendes aus:
   - **IP based matching for Hostname based policy resources**
   - **Case sensitive matching for the Path and Query string components in Web resources**
3. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „Files“

Die Seite **Resource Policies > Files** enthält die folgenden Registerkarten, auf denen Sie eine Dateiressourcenrichtlinie erstellen können.

- „Windows-Registerkarten“ auf Seite 334 – Diese Registerkarte dient zum Erstellen von Windows-Ressourcenrichtlinien wie Richtlinien für den Ressourcenzugriff oder Richtlinien für Windows-Anmeldedaten.
- „Registerkarte „UNIX/NFS““ auf Seite 337 – Diese Registerkarte dient zum Erstellen einer UNIX/NFS-Ressourcenrichtlinie.
- „Registerkarte „Compression““ auf Seite 338 – Diese Registerkarte dient zum Erstellen einer Komprimierungsrichtlinie.
- „Registerkarte „Encoding““ auf Seite 339 – Diese Registerkarte dient zum Festlegen der Codierung für die Internationalisierung von IVE-Datenverkehr.
- „Registerkarte „Options““ auf Seite 340 – Diese Registerkarte dient zum Festlegen von Dateiressourcenoptionen.

Schreiben einer Dateiressourcenrichtlinie

Wenn Sie die Dateizugriffsfunktion für eine Rolle aktivieren, müssen Sie Ressourcenrichtlinien erstellen, die angeben, auf welche Windows- und UNIX/NFS-Ressourcen ein Benutzer zugreifen darf und welche Codierung für die Kommunikation mit Windows- und NFS-Dateifreigaben verwendet werden soll. Wenn ein Benutzer eine Datei anfordert, wertet das IVE die entsprechenden Ressourcenrichtlinien aus, z. B. Ressourcenrichtlinien für den Windows-Zugriff bei einer Anforderung eines MS Word-Dokuments (.doc-Datei). Wenn das IVE für eine Benutzeranforderung einer Ressource, die in der entsprechenden Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer Dateiressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen** – Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Dateirichtlinie müssen Sie Dateiserver oder bestimmte Freigaben angeben. Weitere Informationen finden Sie unter „Angeben von Windows-Dateiressourcen“ auf Seite 333 und „Angeben von UNIX/NFS-Dateiressourcen“ auf Seite 334.
- **Rollen** – Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.

- **Aktionen** – Jeder Ressourcenrichtlinientyp führt eine bestimmte Aktion aus: Zugriff auf eine Ressource gewähren bzw. verweigern oder eine Funktion ausführen bzw. nicht ausführen, z. B. einem Benutzer Schreibzugriff auf ein Verzeichnis gewähren. Sie können auch detaillierte Regeln schreiben, mit denen Sie weitere Bedingungen für eine Benutzeranforderung festlegen. Siehe „Schreiben einer detaillierten Regel“ auf Seite 306.

Für das IVE-Modul, das Ressourcenrichtlinien auswertet, müssen die in der Liste **Resources** einer Richtlinie aufgelisteten Ressourcen wie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305 beschrieben im kanonischen Format aufgeführt sein. In den folgenden Abschnitten werden spezielle Aspekte behandelt, die beim Angeben einer Dateiressource im kanonischen Format beachtet werden müssen.

Angeben von Windows-Dateiressourcen

Kanonisches Format:

\\Server[\Freigabe[\Pfad]]

Die drei Bestandteile sind:

- **Server** (erforderlich) – Mögliche Werte:
  - **Hostname** – Die Systemvariable <Benutzername> kann verwendet werden.
  - **IP-Adresse** – Die IP-Adresse muss in folgendem Format angegeben werden: a.b.c.d

  Die beiden vorangehenden umgekehrten Schrägstriche (\\) sind erforderlich.
- **Freigabe** (optional) – Wenn keine Freigabe angegeben ist, wird von einem Sternchen (*) ausgegangen, was bedeutet, dass ALLE Pfade zutreffen. Die Systemvariable <username> darf verwendet werden.
- **Pfad** (optional) – Sonderzeichen sind zulässig, einschließlich:

Tabelle 19: Sonderzeichen im Pfad

*	Entspricht einem beliebigen Zeichen
%	Entspricht einem beliebigen Zeichen außer dem Schrägstrich (/)
?	Entspricht genau einem Zeichen

Wenn kein Pfad angegeben ist, wird von einem Schrägstrich (/) ausgegangen, d. h., es werden nur die Ordner der obersten Ebene berücksichtigt. Beispiel:

\\%.danastreet.net\share\<username>*
.juniper.com\dana
\\10.11.0.10\share\web*
\\10.11.254.227\public\%.doc

Angeben von UNIX/NFS-Dateiressourcen

Kanonisches Format:

Server[/Pfad]

Die beiden Bestandteile sind:

- **Server** (erforderlich) – Mögliche Werte:
  - **Hostname** – Die Systemvariable <Benutzername> kann verwendet werden.
  - **IP-Adresse** – Die IP-Adresse muss in folgendem Format angegeben werden: a.b.c.d

  Die beiden vorangehenden umgekehrten Schrägstriche (\\) sind erforderlich.
- **Pfad** (optional) – Sonderzeichen sind zulässig, einschließlich:

Tabelle 20: Sonderzeichen im Pfad

*	Entspricht einem beliebigen Zeichen
%	Entspricht einem beliebigen Zeichen außer dem umgekehrten Schrägstrich (\)
?	Entspricht genau einem Zeichen

Wenn kein Pfad angegeben ist, wird von einem umgekehrten Schrägstrich (\) ausgegangen, d. h., es werden nur die Ordner der obersten Ebene berücksichtigt. Beispiel:

%.danastreet.net/share/users/<username>/*
.juniper.com/dana/
10.11.0.10/web/*
10.11.254.227/public/%.txt

Windows-Registerkarten

Registerkarte „Access“

Über die Registerkarte **Windows > Access** können Sie eine Dateiressourcenrichtlinie schreiben, die angibt, auf welche Windows-Ressourcen Benutzer zugreifen dürfen. Für Windows-Ressourcen geben Sie den Server und die Freigabe sowie bei Bedarf den Pfad für einen bestimmten Ordner ein.

Schreiben einer Ressourcenrichtlinie für Windows-Zugriff

So schreiben Sie eine Ressourcenrichtlinie für Windows-Zugriff:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > File > Windows > Access**.
2. Klicken Sie auf der Seite **Windows File Access Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie. (Dies ist optional.)

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Allow access** – Hiermit gewähren Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen. Aktivieren Sie **Read-only**, damit die Benutzer keine Dateien auf dem Server speichern können.
   - **Deny access** – Hiermit verweigern Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen.
   - **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Windows File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Registerkarte „Credentials“

Auf der Registerkarte **Windows > Credentials** können Sie eine Dateiressourcenrichtlinie schreiben, mit der Sie Anmeldeinformationen für das IVE angeben können, die an einen Dateiserver gesendet werden, wenn eine Benutzeranfrage einer Ressource in der Liste **Resource** entspricht. Sie können außerdem das IVE so konfigurieren, dass Benutzer zur Eingabe ihrer Anmeldeinformationen aufgefordert werden.

Schreiben einer Ressourcenrichtlinie für Windows-Anmeldeinformationen

So schreiben Sie eine Ressourcenrichtlinie für Windows-Anmeldeinformationen:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > File > Windows > Credentials**.
2. Klicken Sie auf der Seite **Windows Credentials Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   a. Eine Bezeichnung für diese Richtlinie.
   b. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below** – Die Richtlinie gilt für alle Benutzer mit Ausnahme derer, die den Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Use static credentials** – Diese Option ermöglicht die Angabe statischer Administratoranmeldedaten, die das IVE an die in der Liste **Resources** auf Ordner- und Dateiebene angegebenen Ressourcen sendet. Der IVE-Server für die Dateinavigation hält jedoch die Verbindungen mit einem Server\Freigabe offen, sodass die Verbindung mit einem anderen Ordner auf derselben Freigabe über ein anderes Konto möglicherweise nicht zuverlässig funktioniert. Das IVE maskiert das hier eingegebene Kennwort mit Sternchen.
   - **Use variable credentials** – Diese Option ermöglicht die Angabe variabler Administratoranmeldedaten, die das IVE an die in der Liste **Resources** auf Ordner- und Dateiebene angegebenen Ressourcen sendet. Sie können in diesen Feldern IVE-Variablen wie <USERNAME> und <PASSWORD> sowie eine Domäne eingeben. Beispiel: ihrefirma.net\<BENUTZERNAME>.
   - **Prompt for user credentials** – Wenn für eine Dateifreigabe in einer in der Liste **Resources** angegebenen Ressource Anmeldeinformationen erforderlich sind, vermittelt das IVE die Anfrage, indem eine Authentifizierungsanfrage auf dem IVE angezeigt wird. Der Benutzer muss die Anmeldeinformationen für die Freigabe eingeben, auf die er zugreifen möchte. Wenn die angegebenen Anmeldedaten fehlschlagen, verweigert das IVE dem Benutzer den Zugriff auf die Ressource.

- **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Windows File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Registerkarte „UNIX/NFS“

Über die Registerkarte **UNIX/NFS** können Sie eine Dateiressourcenrichtlinie schreiben, die angibt, auf welche UNIX/NFS-Ressourcen Benutzer zugreifen dürfen. Sie geben UNIX/NFS-Ressourcen an, indem Sie einen Serverhostnamen oder die IP-Adresse eingeben und bei Bedarf den Pfad zu einer bestimmten Freigabe angeben.

Schreiben einer UNIX/NFS-Ressourcenrichtlinie

So schreiben Sie eine UNIX/NFS-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > File > UNIX/NFS**.

2. Klicken Sie auf der Seite **Unix/NFS File Access Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie. (Dies ist optional.)

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.

   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Allow access** – Hiermit gewähren Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen. Aktivieren Sie **Read-only**, damit die Benutzer keine Dateien auf dem Server speichern können.
   - **Deny access** – Hiermit verweigern Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen.
   - **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Unix/NFS File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Registerkarte „Compression“

Geben Sie auf den **Compression**-Registerkarten an, welchen Dateidatentyp das IVE komprimieren soll, wenn Sie auf der Seite **Maintenance > System > Options** der Webkonsole die GZIP-Komprimierung aktivieren.

HINWEIS: Das IVE ist mit zwei Dateikomprimierungsrichtlinien (*:*/*) zur Komprimierung aller entsprechenden Dateidaten vorkonfiguriert. Sie können diese Richtlinien über die Seiten **Resource Policies > Files > Compression** der Webkonsole aktivieren.

Schreiben einer Webkomprimierungsrichtlinie

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Files > Compression**.

2. Geben Sie an, welche Art von Dateidaten komprimiert werden sollen, indem Sie die Registerkarte **Windows** oder **Unix/NFS** wählen.

3. Klicken Sie auf **New Policy**.

4. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

5. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305.

6. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
7. Geben Sie im Bereich **Action** Folgendes an:
   - **Compress** – Das IVE komprimiert die unterstützten Inhaltstypen der angegebenen Ressource.
   - **Do not compress** – Das IVE komprimiert die unterstützten Inhaltstypen der angegebenen Ressource nicht.
   - **Use Detailed Rules** – Hiermit geben Sie detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 306.
8. Klicken Sie auf **Save Changes**.

Registerkarte „Encoding“

Auf der Registerkarte **Files > Encoding** können Sie festlegen, wie das IVE die Daten bei der Interaktion mit Dateiservern codiert.

Angeben der Codierung für die Internationalisierung von IVE-Datenverkehr

So geben Sie die Codierung für die Internationalisierung von IVE-Datenverkehr an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > File > Encoding**.
2. Wählen Sie die entsprechende Option aus:
   - Western European (ISO-8859-1)
   - Simplified Chinese (CP936)
   - Simplified Chinese (GB2312)
   - Traditional Chinese (CP950)
   - Traditional Chinese (Big5)
   - Japanese (Shift-JIS)
   - Korean

3. Klicken Sie auf **Save Changes**.

Registerkarte „Options“

Auf der Registerkarte **Options** können Sie die für Ihre Webressourcenrichtlinien anwendbaren Dateiressourcenoptionen festlegen. Wenn Sie eine Dateiressourcenrichtlinie aktivieren, kompiliert das IVE eine Liste von Hostnamen, die im Feld **Resources** jeder Dateiressourcenrichtlinie angegeben wird. Das IVE wendet die aktivierten Optionen dann auf diese umfassende Liste von Hostnamen an.

Angeben von Dateiressourcenoptionen

So geben Sie eine Dateiressourcenoption an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Files > Options**.

2. Wählen Sie Folgendes aus:

   - **IP based matching for Hostname based policy resources** – Das IVE sucht nach IP-Adressen, die den in einer Dateiressourcenrichtlinie angegebenen Hostnamen entsprechen. Wenn ein Benutzer versucht, auf einen Server zuzugreifen, indem er eine IP-Adresse anstelle des Hostnamens angibt, vergleicht das IVE die IP mit einer zwischengespeicherten Liste von IP-Adressen, um festzustellen, ob ein Hostname mit einer IP übereinstimmt. Wenn eine Übereinstimmung vorliegt, akzeptiert das IVE diese als eine Richtlinienübereinstimmung und führt die für die Ressourcenrichtlinie angegebene Aktion durch.

HINWEIS: Diese Option wird nicht auf Hostnamen angewendet, die Platzhalter und Parameter enthalten.

   - **Case sensitive matching for the Path component in File resources** – Wählen Sie diese Option, wenn Benutzer einen URL unter Berücksichtigung der Groß-/Kleinschreibung für eine NFS-Ressource eingeben sollen. Verwenden Sie diese Option beim Einfügen des Benutzernamens oder des Kennwortes in einen URL.

HINWEIS: Diese Option wird auf Windows-Servern nicht angewendet.

   - **Allow NTLM V1** – Wählen Sie diese Option, um ein Fallback zur Authentifizierung mit NTLM Version 1 zuzulassen, wenn die Kerberos-Authentifizierung von Administratoranmeldedaten fehlschlägt.

3. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „Telnet/SSH“

Mithilfe der Option Secure Terminal Access können Benutzer eine unverschlüsselte Verbindung mit internen Serverhosts über Telnet-Protokolle herstellen oder in einer verschlüsselten SSH-Sitzung (Secure Shell) über eine webbasierte Terminalsitzungs-Emulation kommunizieren. Diese Funktion unterstützt die folgenden Anwendungen und Protokolle:

- Netzwerkprotokolle – Zu den unterstützten Netzwerkprotokollen zählen Telnet und SSH.
- Terminaleinstellungen – Zu den unterstützten Terminaleinstellungen zählen VT100, VT320, Ableitungen und Bildschirmpuffer.
- Sicherheit – Zu den unterstützten Sicherheitsmechanismen zählen Web-/Clientsicherheit mittels SSL und Hostsicherheit (z. B. SSH, sofern erwünscht).

Die Seite **Resource Policies > Telnet/SSH** enthält die folgenden Registerkarten:

- „Registerkarte „Access““ auf Seite 341 – Diese Registerkarte dient zum Erstellen einer Telnet/SSH-Ressourcenrichtlinie.
- „Registerkarte „Options““ auf Seite 343 – Diese Registerkarte dient zum Festlegen der Telnet/SSH-Ressourcenoption.

Registerkarte „Access“

Wenn Sie die Telnet/SSH-Zugriffsfunktion für eine Rolle aktivieren, müssen Sie Ressourcenrichtlinien erstellen, die die für die Benutzer zugänglichen Remoteserver definieren. Wenn das IVE eine Benutzeranforderung einer Ressource in einer Telnet/SSH-Richtlinie zuordnen kann, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer Telnet/SSH-Ressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen** – Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Telnet/SSH-Richtlinie müssen Sie Remoteserver angeben, mit denen Benutzer eine Verbindung herstellen können.
- **Rollen** – Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.
- **Actions** – Eine Telnet/SSH-Ressourcenrichtlinie gewährt oder verweigert den Zugriff auf einen Server.

Für das IVE-Modul, das Ressourcenrichtlinien auswertet, müssen die in der Liste **Resources** einer Richtlinie aufgelisteten Ressourcen wie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 217 beschrieben im kanonischen Format aufgeführt sein.

Schreiben einer Telnet/SSH-Ressourcenrichtlinie

So schreiben Sie eine Telnet/SSH-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Telnet/SSH > Access** aus.
2. Klicken Sie auf der Seite Telnet/SSH **Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   a. Eine Bezeichnung für diese Richtlinie.
   b. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Legen Sie im Abschnitt **Resources** wie unter „Angeben von Serverressourcen“ auf Seite 218 beschrieben die Server fest, für die diese Richtlinie gilt.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles** – Bei Auswahl dieser Option gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles** – Bei Auswahl dieser Option gilt die Richtlinie nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below** – Bei Auswahl dieser Option gilt die Richtlinie für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access** – Hiermit gewähren Sie den Zugriff auf die in der Liste **Resources** aufgeführten Server.
   - **Deny access** – Hiermit verweigern Sie den Zugriff auf die in der Liste **Resources** aufgeführten Server.
   - **Use Detailed Rules** – Wählen Sie diese Option, um detaillierte Regeln für diese Richtlinie festzulegen. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 220.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite Telnet/SSH **Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Registerkarte „Options“

Über die Registerkarte **Options** können Sie die Telnet/SSH-Ressourcenoption so festlegen, dass IP-Adressen mit Hostnamen abgeglichen werden, die in Ihren Telnet/SSH-Ressourcenrichtlinien als Ressourcen angegeben sind. Wenn Sie diese Option aktivieren, sucht das IVE nach IP-Adressen, die den in einer Telnet/SSH-Ressourcenrichtlinie angegebenen Hostnamen entsprechen. Wenn ein Benutzer versucht, auf einen Server zuzugreifen, indem er eine IP-Adresse anstelle des Hostnamens angibt, vergleicht das IVE die IP mit einer zwischengespeicherten Liste von IP-Adressen, um festzustellen, ob ein Hostname mit einer IP übereinstimmt. Wenn eine Übereinstimmung vorliegt, akzeptiert das IVE diese als eine Richtlinienübereinstimmung und führt die für die Ressourcenrichtlinie angegebene Aktion durch.

Wenn Sie diese Option aktivieren, stellt das IVE eine Liste mit Hostnamen zusammen, die im Feld **Resources** der einzelnen Telnet/SHH-Ressourcenrichtlinien angegeben sind. Das IVE wendet die Option dann auf diese umfassende Liste von Hostnamen an.

HINWEIS: Diese Option wird nicht auf Hostnamen angewendet, die Platzhalter und Parameter enthalten.

Angeben der Telnet/SSH-Ressourcenoption

So geben Sie die Telnet/SSH-Ressourcenoption an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Telnet/SSH > Options** aus.

2. Wählen Sie **IP based matching for Hostname based policy resources** aus. Das IVE sucht nach den IP-Adressen, die den Hostnamen in einer Telnet/SSH-Ressourcenrichtlinie entsprechen. Wenn ein Benutzer versucht, auf einen Server zuzugreifen, indem er eine IP-Adresse anstelle des Hostnamens angibt, vergleicht das IVE die IP mit einer zwischengespeicherten Liste von IP-Adressen, um festzustellen, ob ein Hostname mit einer IP übereinstimmt. Wenn eine Übereinstimmung vorliegt, akzeptiert das IVE diese als eine Richtlinienübereinstimmung und führt die für die Ressourcenrichtlinie angegebene Aktion durch.

3. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „Network Connect“

Über die Option Network Connect verfügen Sie auf Netzwerkebene über einen sicheren, SSL-basierten Remotezugriff auf *alle* Unternehmensanwendungsressourcen unter Verwendung des IVE über Port 443.

HINWEIS: Zum Installieren von Network Connect benötigen Benutzer wie unter „Installation von clientseitigen Anwendungen“ auf Seite 411 beschrieben entsprechende Berechtigungen. Wenn dies nicht gegeben ist, müssen Sie zum Umgehen dieser Anforderung den Juniper Installer Service verwenden, der Ihnen auf der Seite **Maintenance > System > Installers** in der Webkonsole zur Verfügung steht.

Die Seite **Resource Policies > Network Connect** enthält die folgenden Registerkarten:

- „Registerkarte „Network Connect Access Control““ auf Seite 344 – Diese Registerkarte dient zum Erstellen einer Ressourcenrichtlinie für den Network Connect-Zugriff.
- „Registerkarte „Network Connect Logging““ auf Seite 345 – Diese Registerkarte dient zum Erstellen einer Richtlinie für die Network Connect-Protokollierung.
- „Registerkarte „Network Connect Connection Profiles““ auf Seite 346 – Diese Registerkarte dient zum Erstellen eines Network Connect-Verbindungsprofils.
- „Registerkarte „Network Connect Split Tunneling““ auf Seite 350 – Diese Registerkarte dient zum Erstellen einer Network Connect-Ressourcenrichtlinie für Netzwerke mit geteilten Tunneln.

Für das IVE-Plattformmodul, das Ressourcenrichtlinien auswertet, müssen die in der Liste **Resources** einer Richtlinie aufgelisteten Ressourcen wie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305 beschrieben im kanonischen Format aufgeführt sein.

Registerkarte „Network Connect Access Control“

Auf der Registerkarte **Network Connect Access Control** können Sie eine Network Connect-Ressourcenrichtlinie zum Steuern der Ressourcen erstellen, mit denen Benutzer bei der Verwendung von Network Connect eine Verbindung herstellen können.

Schreiben einer Ressourcenrichtlinie für Network Connect-Zugriff

So schreiben Sie eine Ressourcenrichtlinie für Network Connect-Zugriff:

1. Wählen Sie in der Webkonsole **Resource Policies > Network Connect > Network Connect Access Control**.
2. Klicken Sie auf der Network Connect-Seite **Network Connect Access Control** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie. (Dies ist optional.)

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Die Richtlinie gilt für alle Benutzer.
   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Allow access** – Hiermit gewähren Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen.
   - **Deny access** – Hiermit verweigern Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen.
   - **Use Detailed Rules** – Wählen Sie diese Option, um Ressourcenrichtlinienregeln zur zusätzlichen Beschränkung der angegebenen Ressourcen zu definieren.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite Network Connect **Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Registerkarte „Network Connect Logging“

Die Registerkarte **Network Connect Logging** dient zum Kompilieren und Anzeigen von Paketinformationen für Network Connect-Benutzer. Die Kompilierung clientseitiger Network Connect-Paketinformationen kann die Unterstützung und Fehlerbehebung für Network Connect-Probleme wie Sitzungsfehler oder von Benutzern gemeldete regelmäßige Paketverluste verbessern. Sie können spezifische Pakettypen basierend auf der Authentifizierung, der Autorisierung und den IP-Zuordnungsinformationen des Benutzers, Quell- und Ziel-IP-Adressen, Quell- und Zielportzuordnungen und Sitzungstransportprotokollen protokollieren und suchen.

Schreiben einer Richtlinie für die Network Connect-Protokollierung

So schreiben Sie eine Richtlinie für die Network Connect-Protokollierung:

1. Wählen Sie in der Webkonsole **Resource Policies > Network Connect > Network Connect Logging**.
2. Klicken Sie auf der Seite **Network Connect Logging** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   a. Eine Bezeichnung für diese Richtlinie.
   b. Eine Beschreibung der Richtlinie (optional).
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 305.
5. Wählen Sie im Abschnitt **Roles** eine der folgenden Optionen:
   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Wählen Sie im Abschnitt **Action** eine der folgenden Optionen aus:
   - **Log Packets** – Bei Auswahl dieser Option protokolliert das IVE automatisch Pakete für alle Verbindungen, die den in der Protokollierungsrichtlinie definierten Kriterien entsprechen.
   - **Use Detailed Rules** – Wählen Sie diese Option, um Ressourcenrichtlinienregeln zur zusätzlichen Beschränkung der angegebenen Ressourcen zu definieren.
7. Klicken Sie auf **Save Changes**.

Registerkarte „Network Connect Connection Profiles“

Die Registerkarte **Network Connect Connection Profiles** dient zum Erstellen eines Network Connect-Ressourcenprofils. Wenn ein IVE eine Clientanforderung zum Starten einer Network Connect-Sitzung empfängt, weist es dem clientseitigen Network Connect-Agent eine IP-Adresse zu. Das IVE weist diese IP-Adresse anhand der Richtlinien für den IP-Adresspool zu, die auf eine Benutzerrolle zutreffen. Darüber hinaus ermöglicht diese Funktion die Angabe des Transportprotokolls, der Verschlüsselungsmethode und der Datenkomprimierung für die Network Connect-Sitzung.

Erstellen eines Network Connect-Verbindungsprofils

So schreiben Sie ein Network Connect-Verbindungsprofil:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Network Connect > Network Connect Connection Profiles**.

2. Klicken Sie auf der Seite **Network Connect Connection Profiles** auf **New Profile**.

3. Geben Sie auf der Seite **New Profile** die folgenden Informationen ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

4. Geben Sie im Abschnitt **IP address assignment** durch Auswahl einer der folgenden Optionen die Methode der clientseitigen IP-Adresszuordnung an:

   - **DHCP server** – Diese Option ermöglicht die Angabe des Hostnamens oder der IP-Adresse eines für die clientseitige IP-Adresszuordnung verantwortlichen DHCP-Servers (Dynamic Host Configuration Protocol) im Netzwerk.

   - **IP address pool** – Diese Option ermöglicht die Angabe von IP-Adressen oder eines IP-Adressbereichs für das IVE zur Zuweisung an Clients, die den Network Connect-Dienst ausführen. Verwenden Sie das kanonische Format: IP_Bereich

     Der IP_Bereich kann im Format a.b.c.d-e angegeben werden, wobei der letzte Bestandteil der IP-Adresse ein durch einen Bindestrich (-) getrennter Bereich ist. Sonderzeichen sind nicht zulässig. Beispiel: 10.10.10.1-100.

HINWEIS: Wir empfehlen, das Netzwerk so einzurichten, dass sich der clientseitige IP-Adresspool von Network Connect oder der im Network Connect-Verbindungsprofil angegebene DHCP-Server in demselben Subnetz befindet wie das IVE.

Wenn Ihre Netzwerktopologie erfordert, dass sich die interne IP-Schnittstelle des IVE und der IP-Adresspool bzw. der DHCP-Server in unterschiedlichen Subnetzen befinden, müssen Sie den Gatewayroutern Ihres Intranets statische Routen hinzufügen. Dadurch wird sichergestellt, dass die Unternehmensressourcen und das IVE einander im internen Netzwerk erreichen können.

5. Legen Sie im Abschnitt **Connection settings** Transport-, Verschlüsselungs- und Komprimierungseinstellungen für dieses Verbindungsprofil fest:

   a. Legen Sie die Einkapselungs- und Transportmethode durch Auswahl einer der folgenden Optionen fest:

      - **ESP (maximize performance)** – Wählen Sie diese Option, um eine UDP-eingekapselte ESP-Übertragungsmethode für die sichere Datenübertragung zwischen dem Client und dem IVE zu verwenden. Die Datenübertragungsparameter können weiter angepasst werden, indem Sie den UDP-Port, Zeitüberschreitungswerte für das ESP-zu-NCP-Fallback und Lebensdauerwerte für den ESP-Verschlüsselungsschlüssel definieren.

      - **oNCP/NCP (maximize compatibility)** – Wählen Sie diese Option, um die standardmäßige oNCP/NCP-Transportmethode für dieses Verbindungsprofil zu verwenden. Hintergrundinformationen zu oNCP, NCP und Optionen für die NCP-Verwendung auf dem IVE finden Sie unter „Registerkarte „NCP““ auf Seite 182.

HINWEIS: Das oNCP-Transportprotokoll bietet im Vergleich zu NCP mehr Flexibilität, da es Macintosh- und Linux-Clients unterstützt. (Das herkömmliche NCP-Transportprotokoll funktioniert in einer reinen Windows-Clientumgebung.) Wenn Sie die automatische oNCP/NCP-Auswahlfunktion auf der Seite **System > Configuration > NCP** der Webkonsole deaktivieren und ein UDP-zu-oNCP/NCP-Failover stattfindet, trennt das IVE die Verbindung von Macintosh- und Linux-Clients, da es von UDP zu NCP wechselt (anstelle von oNCP) und dieses Protokoll diese Benutzer nicht unterstützt.

---

   b. Wenn Sie die Standardwerte des IVE für die **ESP**-Transportmethode übernehmen möchten, fahren Sie mit Schritt c fort. Andernfalls können Sie auch die folgenden Werte angeben:

      - **UDP port** – Geben Sie den IVE-Port an, über den UDP-Verbindungsverkehr geleitet werden soll. Die Standardportnummer lautet 4500.

HINWEIS: Unabhängig davon, ob Sie eine benutzerdefinierte Portnummer angeben oder die im IVE konfigurierte Standardportnummer (4500) übernehmen, müssen Sie auch sicherstellen, dass andere Geräte im verschlüsselten Tunnel UDP-Verkehr zwischen dem IVE und Network Connect-Clients zulassen. Wenn Sie z. B. einen Edge-Router und eine Firewall zwischen dem Internet und Ihrem Firmenintranet verwenden, müssen Sie sicherstellen, dass Port 4500 sowohl im Router als auch der Firewall aktiviert ist und zum Weiterleiten von UDP-Verkehr konfiguriert ist.

      - **ESP to NCP fallback timeout** – Geben Sie einen Zeitraum an (in Sekunden), den das IVE nach einem UDP-Verbindungsausfall abwartet, bevor es automatisch eine Standard-oNCP/NCP-Verbindung herstellt. Der Standardzeitraum ist 15 Sekunden. Wenn Sie einen Wert von 0 Sekunden angeben, führt das IVE nie ein Failover zu einer oNCP/NCP-Verbindung durch.

- **Key lifetime** – Geben Sie den Zeitraum an (in Minuten), während dessen das IVE den gleichen ESP-Verschlüsselungsschlüssel für dieses Verbindungsprofil verwendet. Die lokale Seite und die Remoteseite des verschlüsselten Übertragungstunnels verwenden während eines beschränkten Zeitraums den gleichen Verschlüsselungsschlüssel, um nicht autorisierten Zugriff zu verhindern. Der Standardzeitraum ist 20 Minuten.

HINWEIS: Durch eine häufige Änderung des Verschlüsselungsschlüssels kann der CPU-Overhead im IVE zunehmen.

c. Legen Sie die Verschlüsselungsmethode durch Auswahl einer der folgenden Optionen fest:

- **AES/SHA1 (maximize security)** – Bei Auswahl dieser Option verwendet das IVE während Network Connect-Sitzungen die AES-Verschlüsselung (Advanced Encryption Standard)[1] für den Datenkanal und die SHA1[2]-Authentifizierungsmethode.

- **AES/MD5 (maximize performance)** – Bei Auswahl dieser Option verwendet das IVE während Network Connect-Sitzungen die AES[1]-Verschlüsselung (Advanced Encryption Standard) für den Datenkanal und die MD5[3]-Authentifizierungsmethode.

d. Legen Sie fest, ob eine Komprimierung für die sichere Verbindung verwendet werden soll.

6. Geben Sie im Bereich **Roles** Folgendes an:

- **Policy applies to ALL roles** – Bei Auswahl dieser Option gilt die Richtlinie für alle Benutzer.

- **Policy applies to SELECTED roles** – Bei Auswahl dieser Option gilt die Richtlinie nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

- **Policy applies to all roles OTHER THAN those selected below** – Bei Auswahl dieser Option gilt die Richtlinie für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

1. Die AES-Verschlüsselungsmethode schützt IP-Pakete durch Verschlüsselung mit einem kryptografischen Algorithmus mit 128-Bit-Verschlüsselungsschlüssel.
2. Die SHA1-Authentifizierungsmethode ist leicht zu verwenden und bietet eine effiziente Verschlüsselung von Benutzer-ID- und Kennwortinformationen. Der SHA1-Algorithmus übersetzt die Zeichen, aus denen eine Benutzer-ID oder eine Kennwortzeichenfolge besteht, vor der Übertragung zum oder vom IVE in unlesbaren Text. Der gleiche Algorithmus wird dann verwendet, um die Übersetzung umzukehren, bevor die Zeichenfolgen dem Authentifizierungsserver präsentiert werden.
3. Der MD5-Authentifizierungsalgorithmus erstellt digitale Signaturen. Die MD5-Authentifizierungsmethode übersetzt eine Eingabezeichenfolge (z. B. die ID oder das Anmeldekennwort eines Benutzers) in einen festen 128-Bit-Fingerabdruck (auch bezeichnet als „Message-Digest“), bevor es die Zeichenfolge zum oder vom IVE überträgt.

7. Klicken Sie auf der Seite **New Profile** auf die Registerkarte **DNS**.

8. Aktivieren Sie das Kontrollkästchen **Custom DNS Settings**, um die Standard-DNS-Einstellungen durch die von Ihnen angegebenen Einstellungen zu überschreiben:

   a. **Primary DNS** – Geben Sie die IP-Adresse für den primären DNS-Server an.

   b. **Secondary DNS** – Geben Sie die IP-Adresse für den sekundären DNS-Server an.

   c. **DNS Domain(s)** – Geben Sie die DNS-Domäne(n) an, z. B. „ihrefirma.com“ oder „ihrefirma.net“.

9. Wählen Sie im Abschnitt **DNS search order** die DNS-Serversuchreihenfolge nur dann aus, wenn die Funktion für geteilte Tunnel aktiviert ist:

   - **Search IVE DNS servers first, then client**
   - **Search client DNS first, then IVE**

10. Klicken Sie auf der Seite **New Profile** auf die Registerkarte **DNS**.

11. Wählen Sie im Abschnitt **Network Connect proxy server configuration** eine der folgenden Optionen aus:

    - **No proxy server** – Legt fest, dass das neue Profil keinen Proxyserver erfordert.
    - **Automatic (PAC file on IVE)** – Geben Sie die IP-Adresse des Servers an, auf dem sich die PAC-Datei befindet, oder navigieren Sie zum Speicherort der PAC-Datei auf einem lokalen Host, und laden Sie die Datei in das IVE.
    - **Automatic (PAC file on another server)** – Geben Sie die IP-Adresse des Servers an, auf dem sich die PAC-Datei befindet.
    - **Manual configuration** – Geben Sie die IP-Adresse des Servers und die Portzuordnung an.

12. Klicken Sie auf **Save Changes**.

13. Ordnen Sie die Profile auf der Seite **NC Connection Profiles** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Wenn das IVE die von einem Benutzer angeforderte Ressource einer Ressource in der Liste **Resource** eines Profils (oder einer ausführlichen Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Registerkarte „Network Connect Split Tunneling“

Auf der Registerkarte **Network Connect Split Tunneling** können Sie eine Network Connect-Ressourcenrichtlinie erstellen, die Kombinationen von Netzwerk-IP-Adressen/Netzmasken definiert, für die das IVE Datenverkehr zwischen dem Remoteclient und dem Firmenintranet verarbeitet.

Wenn geteilte Tunnel verwendet werden, ändert Network Connect Routen auf Clients, damit an das Firmenintranet gerichteter Verkehr an Network Connect und jeder weitere Verkehr über den lokalen physischen Adapter geleitet wird. Das IVE versucht, alle DNS-Anforderungen zunächst über den physischen Adapter aufzulösen, und leitet anschließend die fehlgeschlagenen Anforderungen an den Network Connect-Adapter weiter.

Schreiben einer Network Connect-Ressourcenrichtlinie für Netzwerke mit geteilten Tunneln

So schreiben Sie eine Network Connect-Ressourcenrichtlinie für Netzwerke mit geteilten Tunneln:

1. Wählen Sie in der Webkonsole **Resource Policies > Network Connect > Network Connect Split Tunneling**.

2. Klicken Sie auf der Network Connect-Seite **Network Connect Split Tunneling** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:

   a. Eine Bezeichnung für diese Richtlinie.

   b. Eine Beschreibung der Richtlinie (optional).

4. Legen Sie im Abschnitt **Resources** Kombinationen von IP-Adressen/Netzmasken fest, für die das IVE Datenverkehr zwischen dem Remoteclient und dem Firmenintranet verarbeitet. Sie können diese Netzwerke auch in der Schreibweise mit '/' (Schrägstrich) angeben.

5. Geben Sie im Bereich **Roles** Folgendes an:

   - **Policy applies to ALL roles** – Hiermit gilt die Richtlinie für alle Benutzer.

   - **Policy applies to SELECTED roles** – Die Richtlinie gilt nur für Benutzer, die Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

   - **Policy applies to all roles OTHER THAN those selected below** – Diese Richtlinie gilt für alle Benutzer *mit Ausnahme* derer, die den Rollen in der Liste **Selected roles** zugewiesen sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:

   - **Allow access** – Hiermit gewähren Sie den Zugriff auf die in der Liste **Resources** aufgeführten Ressourcen.

   - **Use Detailed Rules** (nach dem Klicken auf **Save Changes** verfügbar) – Wählen Sie diese Option, um Ressourcenrichtlinienregeln zur zusätzlichen Beschränkung der angegebenen Ressourcen zu definieren.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite Network Connect **Split Tunneling Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Verwendungsbeispiel: Konfiguration von Network Connect-Ressourcenrichtlinien

Dieser Abschnitt beschreibt ein reales Verwendungsbeispiel für Network Connect und die erforderlichen Schritte zum Konfigurieren der entsprechenden Ressourcenrichtlinie, mit der Remotebenutzern Zugriff auf das Netzwerk gewährt wird.

Große Finanzinstitute (auch bezeichnet als „Fortune-Companies“) benötigen eine stabile Clientanmeldungsanwendung wie Network Connect, um Mitarbeitern an Remotestandorten eine nahtlose Netzwerkverbindung mit vielen Unternehmensressourcen in der Firmenzentrale bereitzustellen. Häufig müssen Remotebenutzer auf ihren Laptops/Clientcomputern auf mehrere Anwendungen zugreifen, die weit über einfache E-Mail- oder Konferenzplanungsanwendungen hinaus gehen. Diese Remote-„Superuser“ oder „Poweruser“ benötigen sicheren verschlüsselten Zugriff auf leistungsstarke Serveranwendungen wie Microsoft Outlook™, Oracle™-Datenbanken und das Remedy™-Verwaltungssystem.

Für dieses Szenario gehen wir von Folgendem aus:

- Eine kleine Gruppe von Remotebenutzern greift über das gleiche IVE auf die Unternehmensressourcen des Finanzinstituts zu.
- Der Benutzer-ID aller Benutzer ist die gleiche Rolle „user_role_remote“ zugewiesen.
- Host Checker und Cache Cleaner sind konfiguriert und überprüfen die Computer der Benutzer nach der Anmeldung an IVE und dem Start der Network Connect-Sitzungen.
- Alle Benutzer benötigen Zugriff auf drei große Server in der Firmenzentrale mit folgenden Attributen:
  - „outlook.acme.com“ an der IP-Adresse 10.2.3.201
  - „oracle.financial.acme.com“ an der IP-Adresse 10.2.3.202
  - „case.remedy.acme.com“ an der IP-Adresse 10.2.3.99
- Da die Firma eine strikte Verwaltung ihres IP-Adresspools wünscht, stellt jedes IVE IP-Adressen für Remotebenutzer bereit (unser spezielles IVE steuert die IP-Adressen zwischen 10.2.3.128 und 10.2.3.192)
- Die Firma wünscht maximale Sicherheit für den Zugriff und möglichst geringe Clientausfallzeiten.

So konfigurieren Sie eine Network Connect-Ressourcenrichtlinie, die den Remotebenutzern des Finanzinstituts entsprechenden Zugriff gewährt:

1. Erstellen Sie wie unter „Schreiben einer Ressourcenrichtlinie für Network Connect-Zugriff“ auf Seite 344 beschrieben eine neue Network Connect-Ressourcenrichtlinie, in der Sie die drei Server angeben, auf die Remotebenutzer zugreifen sollen:

   a. Geben Sie im Abschnitt **Resources** die für den Zugriff auf die drei Server erforderlichen IP-Adressbereiche durch Wagenrücklauf getrennt an („outlook.acme.com“, „oracle.financial.acme.com“ und „case.remedy.acme.com“).

      udp://10.2.3.64-127:80,443

      udp://10.2.3.192-255:80,443

   b. Aktivieren Sie im Abschnitt Roles die Option **Policy applies to SELECTED roles**, und vergewissern Sie sich, dass die Liste **Selected roles** nur die Rolle „user_role_remote“ enthält.

   c. Aktivieren Sie unter **Action** die Option **Allow access**.

2. Erstellen Sie wie unter „Erstellen eines Network Connect-Verbindungsprofils“ auf Seite 347 beschrieben ein neues Network Connect-Verbindungsprofil, in dem Sie die Transport- und Verschlüsselungsmethode für den Datentunnel zwischen den Clients und dem IVE definieren:

   a. Aktivieren Sie im Abschnitt **IP address assignment** die Option **IP address pool**, und geben Sie 10.2.3.128-192 ins zugehörige Textfeld ein.

   b. Wählen Sie unter **Connection Settings** die Transportoption **ESP** und die Verschlüsselungsoption **AES/SHA1** aus.

   c. Aktivieren Sie im Abschnitt Roles die Option **Policy applies to SELECTED roles**, und vergewissern Sie sich, dass die Liste **Selected roles** nur die Rolle „user_role_remote“ enthält.

Konfigurieren der Seite „Email Client“

Die Secure Email Client-Option ermöglicht Remotebenutzern über einen Webbrowser und eine Internetverbindung den Zugriff auf standardbasierte E-Mail-Anwendungen wie Outlook Express, Netscape Communicator oder Eudora von Qualcomm. Weitere Informationen finden Sie unter „E-Mail-Client – Übersicht“ auf Seite 106.

Wenn Sie die E-Mail-Client-Zugriffsfunktion für eine Rolle aktivieren, müssen Sie eine Ressourcenrichtlinie erstellen, die Einstellungen für den Mailserver angibt. Im Gegensatz zu anderen Zugriffsfunktionen verfügt Secure Email Client nur über eine Ressourcenrichtlinie, die für alle Rollen gilt, für die diese Funktion aktiviert ist. Wenn Sie den E-Mail-Client-Dienst für Benutzer aktivieren, müssen Sie IMAP-, POP- und SMTP-Mailserverinformationen und Einstellungen für die Benutzerauthentifizierung angeben. Das IVE fungiert als E-Mail-Proxy für den bzw. die angegebenen Server.

Das IVE unterstützt mehrere Mailserver. Sie können festlegen, dass alle Benutzer einen Standardmailserver verwenden müssen, oder Sie können Benutzern die Möglichkeit geben, einen benutzerdefinierten SMTP- und IMAP- bzw. POP-Mailserver anzugeben. Wenn Sie Benutzern das Festlegen eines benutzerdefinierten Mailservers ermöglichen, müssen diese die Servereinstellungen über das IVE vornehmen. Das IVE verwaltet die E-Mail-Benutzernamen, um Namenskonflikte zu vermeiden.

Schreiben einer Email Client-Ressourcenrichtlinie für Mailserver

So schreiben Sie eine Email Client-Ressourcenrichtlinie für Mailserver:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Email Client**.
2. Klicken Sie unter **Email Client Support** auf **Enabled**.
3. Wählen Sie unter **Email Authentication Mode** eine der folgenden Optionen aus:
   - **Web-based email session** – Benutzer müssen ein einmaliges E-Mail-Setup für das IVE ausführen. Anschließend konfigurieren sie ihren E-Mail-Client so, dass der Benutzername und das Kennwort verwendet werden, die durch die E-Mail-Einrichtung für das IVE generiert werden. Es empfiehlt sich, dass die Benutzer sich an dem IVE anmelden, um eine E-Mail-Sitzung zu starten. (Standardeinstellung.)
   - **Combined IVE and mail server authentication** – Benutzer konfigurieren ihren E-Mail-Client zur Verwendung der folgenden Anmeldedaten:

- **Username** – Der normale Benutzername eines Benutzers für den Mailserver oder ein Benutzername, der beim E-Mail-Setup für das IVE generiert wird, wenn eine der folgenden Bedingungen zutrifft:
  – der Benutzer verfügt über mehrere Benutzernamen für den Mailserver
  – die Benutzernamen auf dem IVE und dem Mailserver sind unterschiedlich

- **Password** – Das IVE-Kennwort des Benutzers, gefolgt von einem benutzerdefinierbaren Trennzeichen für Anmeldeinformationen, gefolgt von dem Mailserverkennwort des Benutzers.

Benutzer müssen sich nicht am beim IVE anmelden, um E-Mail zu verwenden.

- **Mail server authentication only**– Benutzer konfigurieren ihren E-Mail-Client so, dass ihre normalen Mailserver-Benutzernamen und -Kennwörter verwendet werden. Benutzer müssen sich nicht am IVE anmelden, um E-Mail zu verwenden oder zu konfigurieren.

HINWEIS: Die Benutzer können ihre Benutzernamen und Kennwörter für E-Mail problemlos auf der Seite **Email Setup** ermitteln.

4. Geben Sie unter **Default Server Information** Ihre Mailserverdaten an. Das IVE fungiert als E-Mail-Proxy für diesen Server.

HINWEIS: Sie können nur einen Standardmailserver angeben. Wenn Benutzer E-Mail-Nachrichten von mehreren SMTP- und POP- bzw. IMAP-Servern abrufen müssen, bieten Sie ihnen durch Aktivieren des entsprechenden Kontrollkästchens die Möglichkeit, weitere Mailserver zu definieren. Wenn Sie Benutzern die Festlegung benutzerdefinierter Server ermöglichen, müssen die Benutzer diese Informationen auf ihrer IVE-Seite **Email Setup** eingeben.

5. Geben Sie unter **Email Session Information** Folgendes an:

   - Einen **Idle Timeout**-Wert, der angibt, wie lange sich die E-Mail-Sitzung eines Benutzers im Leerlauf befinden kann, bevor das IVE die E-Mail-Sitzung beendet.

   - Einen Wert für **Max. Session Length**, der angibt, wie lange sich die E-Mail-Sitzung eines Benutzers im Leerlauf befinden kann, bevor das IVE die E-Mail-Sitzung beendet.

6. Klicken Sie auf **Save Changes**.

Kapitel 11

Wartungseinstellungen

Auf der Webkonsole können Sie mithilfe der Einstellungen im Abschnitt **Maintenance** das IVE verwalten und Fehler beheben.

Inhalt

- „Konfigurieren der Seite „System““ auf Seite 359
- „Konfigurieren der Seite „Import/Export““ auf Seite 364
- „Konfigurieren der Seite „Archiving““ auf Seite 376
- „Konfigurieren der Seite „Troubleshooting““ auf Seite 378

Konfigurieren der Seite „System“

Die Seite **System** enthält die folgenden Registerkarten:

- „Registerkarte „Platform““ auf Seite 359 – Auf dieser Registerkarte können Sie neu starten, neu booten, herunterfahren oder die Serververbindung testen.
- „Registerkarte „Upgrade/Downgrade““ auf Seite 360 – Mit Hilfe dieser Registerkarte können Sie ein Juniper Softwaredienstpaket installieren.
- „Registerkarte „Options““ auf Seite 361 – Auf dieser Registerkarte können Sie die Versionsüberwachung aktivieren.
- „Registerkarte „Installers““ auf Seite 361 – Mit Hilfe dieser Registerkarte können Sie eine Anwendung oder einen Dienst herunterladen.

Registerkarte „Platform“

Die Seite **Platform** enthält Secure Access 700-Systemdaten sowie Steuerelemente zum Neustarten, Neubooten oder Herunterfahren eines Secure Access 700. Des Weiteren enthält sie ein Steuerelement zum Testen der Serververbindung.

So wird neu gestartet, neu gebootet, heruntergefahren oder die Serververbindung getestet

Die Seite **Platform** enthält die folgenden Systemdaten für ein IVE:

- **Model** – Zeigt das Modell des IVE an.
- **Version** – Zeigt die IVE-Softwareversion an.
- **Rollback** – Zeigt die Softwareversion an, auf die das IVE beim Ausführen eines Rollbacks des installierten Bildes zurückgesetzt wird.
- **Last Reboot** – Zeigt an, wie viel Zeit seit dem letzten Neubooten des IVE vergangen ist.

Die Seite **Platform** enthält die folgenden Steuerelemente:

- **Restart Services** – Beendet alle Prozesse und startet das Secure Access 700 neu.
- **Reboot** – Schaltet das IVE aus und wieder ein und bootet das Secure Access 700 neu.
- **Shut down** – Fährt das Secure Access 700 herunter, wobei Sie den Reset-Schalter an der Appliance drücken müssen, um den Server neu zu starten. Beachten Sie, dass das Gerät nach dem Herunterfahren des Servers eingeschaltet bleibt.
- **Rollback** – Führt ein Rollback des Softwarebildes durch und startet das IVE neu. Nach dem Neubooten des IVEs wird das Bild des IVEs automatisch auf das im Feld **Rollback** (oben) angezeigte Bild zurückgesetzt.

- **Test Connectivity** – Sendet einen ICMP-Ping-Befehl vom IVE an alle Server, die vom IVE gemäß der Konfiguration verwendet werden, und testet ihre Verbindung. Der Status der einzelnen Server wird unter **Server Connectivity Results** aufgeführt.

HINWEIS: Wenn Sie die Einstellungen auf die werkseitige Konfiguration oder das System in den vorigen Zustand zurücksetzen wollen, schlagen Sie nach unter „Verwenden der seriellen Konsole der IVE-Appliance“ auf Seite 389.

Registerkarte „Upgrade/Downgrade“

Sie installieren ein anderes Dienstpaket, indem Sie zuerst von der Juniper-Support-Website die Software herunterladen und diese dann über die Webkonsole hochladen. Paketdateien werden verschlüsselt und signiert, sodass der IVE-Server nur gültige, von Juniper Networks ausgegebene Pakete akzeptiert. Mit dieser Maßnahme wird verhindert, dass der IVE-Server als „Trojanische Pferde“ bezeichnete Programme akzeptiert.

Dieses Feature wird meist dazu verwendet, Aktualisierungen auf neuere Versionen der Systemsoftware durchzuführen. Sie können jedoch mit diesem Verfahren die Systemsoftware auch auf eine ältere Version herunterstufen oder alle aktuellen Konfigurationseinstellungen löschen und eine neue Ausgangsbasis schaffen. Ein Rollback zu einem vorherigen Systemzustand ist auch über die serielle Konsole möglich. Dieser Vorgang ist unter „Rollback zu einem vorherigen Systemzustand“ auf Seite 390 beschrieben.

HINWEIS: Die Installation eines neuen Dienstpakets kann einige Minuten dauern. Das IVE muss anschließend neu gestartet werden. Da bei diesem Vorgang die vorhandenen Systemdaten gesichert werden, lässt sich die Installationsdauer verkürzen, indem der Inhalt des Systemprotokolls vor der Installation eines Dienstpakets gelöscht wird.

Installieren eines Juniper-Softwaredienstpakets

Exportieren Sie vor der Installation eines neuen Dienstpakets die aktuelle Systemkonfiguration, die lokalen Benutzerkonten, die angepassten Benutzereinstellungen und die Rollen- und Richtlinieninformationen, wie unter „Konfigurieren der Seite „Import/Export““ auf Seite 364 erläutert.

So installieren Sie ein Dienstpaket:

1. Navigieren Sie zur Juniper-Support-Website, und rufen Sie das gewünschte Dienstpaket ab.

2. Wählen Sie in der Webkonsole die Option **Maintenance > System > Upgrade/Downgrade** aus.

3. Klicken Sie auf **Browse**, um das von der Supportsite heruntergeladene Dienstpaket auf der Festplatte zu suchen. Wenn Sie die aktuellen Konfigurationseinstellungen löschen, aber weiterhin dieselbe IVE-Version verwenden möchten, wählen Sie das derzeit in Ihrer Appliance installierte Dienstpaket aus.

4. Wenn Sie die Software auf ein älteres Dienstpaket herunterstufen oder die Konfigurationseinstellungen löschen, wählen Sie **Delete all system and user data**.

HINWEIS: Wenn Sie das IVE zurücksetzen und mit dieser Option alle System- und Benutzerdaten aus der Appliance löschen möchten, müssen Sie vor der erneuten Systemkonfiguration die Netzwerkverbindungen wiederherstellen.

5. Wählen Sie die Dienstpaketdatei aus, und klicken Sie auf **Install Now**.

Registerkarte „Options“

Damit das System auf dem neuesten Stand und sicher bleibt, können Sie sich vom IVE automatisch über wichtige Softwarepatches und -aktualisierungen benachrichtigen lassen. Hierzu werden Juniper Networks die folgenden Daten mitgeteilt: Name Ihrer Firma, MD5-Hash Ihrer Lizenzeinstellungen und Informationen zur aktuellen Softwareversion.

Aktivieren der Versionsüberwachung

So aktivieren Sie automatische Aktualisierungen und Beschleunigerkarten:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > System > Options**.

2. Aktivieren Sie das Kontrollkästchen **Automatic Version Monitoring**, um automatisch über wichtige Softwarepatches und -aktualisierungen benachrichtigt zu werden.

HINWEIS: Zum Schutz Ihres Systems wird dringend empfohlen, diesen automatischen Dienst zu aktivieren. Falls nötig, können Sie ihn jedoch auch deaktivieren.

3. Legen Sie mithilfe der Dropdownliste **End-user Localization** fest, in welcher Sprache die Endbenutzerschnittstelle angezeigt wird (optional). Wenn Sie keine Sprache angeben, wird die Sprache der Endbenutzeroberfläche basierend auf den Browsereinstellungen gewählt.

4. Klicken Sie auf **Save Changes**.

Registerkarte „Installers“

Auf der Registerkarte **Installers** finden Sie zahlreiche Anwendungen und Dienste zum Herunterladen. Sie können Anwendungen oder Dienste als ausführbare Windows-Datei herunterladen, mit der Sie folgende Möglichkeiten haben:

- Verteilen der Datei auf mehrere Clientcomputer mithilfe von Softwareverteilungstools. Mit dieser Option können Sie Anwendungen oder Dienste auf Clientcomputern installieren, deren Benutzer nicht über die zum Installieren von Anwendungen oder Diensten erforderlichen Administratorberechtigungen verfügen.

- Bereitstellen der ausführbaren Datei in einem sicheren Repository, damit Benutzer mit den erforderlichen Administratorrechten die richtige Version herunterladen und installieren können.

Mit diesen Optionen können Sie steuern, welche Version einer Anwendung oder eines Dienstes auf Clientcomputern ausgeführt wird.

Herunterladen von Anwendungen oder Diensten

Die Seite **Installers** enthält die folgenden Steuerelemente:

- **Juniper Installer Service** – Mithilfe des Juniper Installer Service können Benutzer auf dem Client Anwendungen herunterladen, installieren, aktualisieren und ausführen, ohne über Administratorrechte zu verfügen. Zum Ausführen dieser Vorgänge (für die Administratorberechtigungen erforderlich sind), wird der Juniper Installer Service unter dem lokalen Systemkonto des Clients ausgeführt (ein Konto mit vollem Systemzugriff) und automatisch unter Windows Service Control Manager (SCM) registriert. Ein im Webbrowser des Benutzers ausgeführtes Active-X-Steuerelement oder Java Applet übermittelt die Details der auszuführenden Installationsprozesse über einen sicheren Kanal zwischen dem IVE und dem Clientsystem.

HINWEIS: Beachten Sie beim Installieren des Juniper Installer Service auf Clientsystemen Folgendes:

- Sie müssen für die Installation des Juniper Installer Service über Administratorrechte verfügen.
- Stellen Sie vor der Installation von Juniper Installer Service sicher, dass Microsoft Windows Installer auf dem Clientsystem existiert.
- Da Juniper Installer Service Microsoft Windows Installer verwendet, kann Ihre Firma von eventuell verwendeten automatischen Push-Systemen (einschließlich SMS und Install Wrappers) profitieren.
- Der Dienst wird automatisch bei der Installation und während des Clientssystemstarts gestartet.
- Er wird in der Liste der lokalen Dienste als Neoteris Setup Service angezeigt.

- **Hostprüfung** – Clientseitiger Agent, der Endpunktsicherheitsprüfungen an Hosts durchführt, die mit dem IVE eine Verbindung herstellen.

HINWEIS: Wenn Sie Host Checker bereitstellen möchten, deaktivieren Sie auf der Seite **Signing In > End Point > Host Checker** die Option **Auto-upgrade Host Checker** (siehe „Festlegen von allgemeinen Host Checker-Optionen“ auf Seite 206). Andernfalls lädt das IVE die Host Checker-Anwendung auf einen Benutzercomputer herunter, und bei dieser Version kann es sich um eine andere Version als die bereitgestellte handeln.

- **Network Connect** – Diese Option stellt eine clientlose VPN-Verbindung bereit, die als zusätzlicher Fernzugriffsmechanismus auf Unternehmensressourcen unter Verwendung von IVE verwendet werden kann.

So laden Sie Anwendungen oder Dienste herunter:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > System > Installers** aus.

2. Klicken Sie auf den Link **Download** rechts neben dem Dienst oder der Anwendung, die Sie herunterladen möchten. Das Dialogfeld **File Download** wird angezeigt.

3. Klicken Sie im Dialogfeld **File Download** auf die Schaltfläche **Save**. Das Dialogfeld **Save As** wird angezeigt.

4. Geben Sie im Dialogfeld **Save As** den gewünschten Speicherort an.

5. Klicken Sie im Dialogfeld **Save As** auf die Schaltfläche **Save**.

Konfigurieren der Seite „Import/Export“

Die Seite **Import/Export** enthält die folgenden Registerkarten:

- „Registerkarte „Configuration““ auf Seite 364 – Auf dieser Registerkarte können Sie IVE-Konfigurationsdateien, die System- und Netzwerkeinstellungen enthalten, exportieren und importieren.
- „Registerkarte „User Accounts““ auf Seite 365 – Auf dieser Registerkarte können Sie lokale Benutzerkonten importieren oder exportieren.
- „Registerkarte „XML Import/Export““ auf Seite 366 – Auf dieser Registerkarte können Sie XML-Dateien, die Systemeinstellungen enthalten, importieren und exportieren.
- „XML Import/Export – Gebrauchsfälle“ auf Seite 370 – In diesen Gebrauchsfällen finden Sie weitere Informationen zur Verwendung der XML-Import-/Exportfunktion.

Registerkarte „Configuration“

Auf dieser Registerkarte können Sie IVE-Konfigurationsdateien, die System- und Netzwerkeinstellungen enthalten, exportieren und importieren. Die Beschreibung dazu finden Sie in „Importieren und Exportieren von IVE-Konfigurationsdateien“ auf Seite 130.

HINWEIS: Wenn Sie Ressourcenrichtlinien exportieren möchten, exportieren Sie Benutzerkonten. Weitere Informationen finden Sie unter „Registerkarte „User Accounts““ auf Seite 365.

Exportieren einer Systemkonfigurationsdatei

So exportieren Sie eine Systemkonfigurationsdatei

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Configuration**.
2. Geben Sie unter **Export** ein Kennwort ein, wenn die Konfigurationsdatei durch ein Kennwort geschützt werden soll.
3. Klicken Sie zum Speichern der Datei auf **Save Config As**.

Importieren einer Systemkonfigurationsdatei

So importieren Sie eine Konfigurationsdatei

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Configuration**.
2. Geben Sie an, ob Sie das IVE-Serverzertifikat importieren möchten. Das Zertifikat wird nur importiert, wenn Sie das Kontrollkästchen **Import IVE Certificate(s)?** aktivieren.

3. Wählen Sie eine der folgenden Importoptionen aus:

   - **Import everything (except IVE Certificate(s))** – Diese Option importiert alle Konfigurationseinstellungen, mit Ausnahme von IVE-Serverzertifikaten.

   - **Import everything but the IP address** – Diese Option schließt lediglich die IP-Adresse aus der importierten Konfigurationsdatei aus. Wenn Sie die IP-Adresse ausschließen, wird die IP-Adresse des Servers beim Importieren der Datei nicht geändert.

   - **Import everything except network settings** – Diese Option importiert alle Konfigurationseinstellungen mit Ausnahme der Netzwerkeinstellungen. Wenn Sie die Netzwerkeinstellungen ausschließen, werden die Informationen auf der Seite **System > Network** (Einstellungen für internen Port, externen Port und statische Routen) beim Importieren der Datei nicht geändert.

   - **Import only Server Certificate(s)** – Diese Option importiert lediglich die IVE-Serverzertifikate. Achten Sie darauf, dass das Kontrollkästchen **Import IVE Certificate(s)?** aktiviert ist, wenn Sie diese Option verwenden.

4. Wechseln Sie zu der Konfigurationsdatei, die in der Standardeinstellung system.cfg heißt.

5. Geben Sie das für die Datei festgelegte Kennwort ein. Wenn Sie vor dem Export der Datei kein Kennwort festgelegt haben, lassen Sie dieses Feld leer.

6. Klicken Sie auf **Import Config**.

Registerkarte „User Accounts“

Auf dieser Registerkarte können Sie lokale Benutzerkonten und Ressourcenrichtlinien exportieren oder importieren. Die Beschreibung dazu finden Sie in „Importieren und Exportieren von IVE-Konfigurationsdateien“ auf Seite 130.

Lokale Benutzerkonten oder Ressourcenrichtlinien exportieren

So exportieren Sie lokale Benutzerkonten oder Ressourcenrichtlinien:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > User Accounts**.

2. Geben Sie unter **Export** ein Kennwort ein, wenn die Konfigurationsdatei durch ein Kennwort geschützt werden soll.

3. Klicken Sie zum Speichern der Datei auf **Save Config As**.

Lokale Benutzerkonten oder Ressourcenrichtlinien importieren

So importieren Sie lokale Benutzerkonten oder Ressourcenrichtlinien:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > User Accounts**.

2. Wechseln Sie zu der Konfigurationsdatei, die in der Standardeinstellung user.cfg heißt.

3. Geben Sie das für die Datei festgelegte Kennwort ein. Wenn Sie vor dem Export der Datei kein Kennwort festgelegt haben, lassen Sie dieses Feld leer.

4. Klicken Sie auf **Import Config**.

Registerkarte „XML Import/Export“

Auf den Seiten **Maintenance > Import/Export > XML Import/Export** können Sie eine XML-Konfigurationsdatei, die ausgewählte Einstellungen enthält, aus einem IVE exportieren und sie anschließend in dasselbe oder ein anderes IVE importieren. Eine Beschreibung dazu finden Sie in „Importieren und Exportieren von XML-Konfigurationsdateien“ auf Seite 130.

XML-Konfigurationsdaten exportieren

So exportieren Sie XML-Konfigurationsdaten:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > XML Import/Export > Export** aus.

2. Klicken Sie unter **Schema Files** auf den Link, um die XML-Schemadateien (.xsd) herunterzuladen, die die IVE-Objekte beschreiben (optional). Weitere Informationen zu Schemadateien finden Sie unter „Herunterladen von Schemadateien“ auf Seite 141.

3. Klicken Sie zum Exportieren aller auf der Seite angegebenen Einstellungen auf die Schaltfläche **Select All**. Andernfalls wählen Sie die spezifischen zu exportierenden Informationen aus:

   - Aktivieren Sie das Kontrollkästchen **Export Network Settings and Licenses**, um Netzwerkeinstellungen einschließlich der internen und externen Porteinstellungen sowie der Lizenzinformationen zu exportieren.

HINWEIS: Die folgenden Regeln gelten für exportierte und importierte Lizenzen:

- Die exportierten Lizenzdaten sind verschlüsselt und können daher nicht bearbeitet werden.

- Ein XML-Import von Lizenzen ist nur gültig, wenn auf dem für den Import der Lizenz verwendeten Gerät zurzeit keine Lizenz installiert ist. Ist bereits eine Lizenz installiert, werden alle importierten Lizenzen gelöscht. Wenn Sie dennoch eine Lizenz importieren möchten, müssen Sie das IVE auf die Werkseinstellungen zurücksetzen und anschließend den Import durchführen.

- Wird nach dem Löschen einer temporären Lizenz vom IVE eine Lizenz importiert, wird die importierte Lizenz verworfen, da die gelöschte Lizenz noch immer aktiviert werden kann und die Importfunktion versucht, alle derzeit auf dem IVE vorhandenen Lizenzdaten zu erhalten.

- Aktivieren Sie das Kontrollkästchen **Sign-in Settings**, um Anmelde-URLs, standardmäßige Anmeldeseiten und Authentifizierungsserver zu exportieren.

  Wählen Sie im Abschnitt **Sign-in URLs** eine der folgenden Optionen:

  - Wählen Sie zum Exportieren aller Anmelde-URLs die Option **ALL sign-in URLs** aus.
  - Aktivieren Sie **SELECTED sign-in URLs**, wählen Sie in der Liste **Available Sign-in URLs** URLs aus, und klicken Sie zum Exportieren dieser ausgewählten URLs auf **Add**.

  Wählen Sie im Abschnitt **Sign-in Pages** eine der folgenden Optionen:

  - Wählen Sie zum Exportieren aller Anmeldeseiten **ALL Pages** aus.
  - Wählen Sie **ONLY pages used by URLs selected above** aus, um die exportierten Seiten auf jene zu beschränken, die für die von Ihnen gewählten Anmelde-URLs gültig sind.
  - Klicken Sie auf **SELECTED pages...**, und wählen Sie anschließend in der Liste **Available Pages** Seiten aus. Klicken Sie auf **Add**, wenn Sie nur diese Seiten exportieren möchten.

  Wählen Sie im Abschnitt **Authentication servers** eine der folgenden Optionen:

  - Wählen Sie zum Exportieren aller Authentifizierungsserver **ALL auth servers** aus.
  - Aktivieren Sie **SELECTED auth servers...**, wählen Sie in der Liste **Available Servers** Server aus, und klicken Sie zum Exportieren dieser ausgewählten Server auf **Add**.

- Aktivieren Sie zum Exportieren von Authentifizierungsbereichen das Kontrollkästchen **Export Authentication Realms**.

  Wählen Sie im Abschnitt **Administrator Realms** eine der folgenden Optionen:

  - Wählen Sie zum Exportieren aller Administratorbereiche die Option **ALL admin realms**.
  - Klicken Sie auf **SELECTED admin realms...**, und wählen Sie anschließend in der Liste **Available Realms** Bereiche aus. Klicken Sie auf **Add**, wenn Sie nur diese Bereiche exportieren möchten.

  Wählen Sie im Abschnitt **User Realms** eine der folgenden Optionen:

  - Wählen Sie zum Exportieren aller Benutzerbereiche die Option **ALL user realms**.

- Klicken Sie auf **SELECTED user realms...**, und wählen Sie anschließend in der Liste **Available Realms** Bereiche aus. Klicken Sie auf **Add**, wenn Sie nur diese Bereiche exportieren möchten.

- Aktivieren Sie zum Exportieren von Rollenzuordnungsregeln das Kontrollkästchen **Export Roles**.

  Wählen Sie im Abschnitt **Delegated Admin Roles** eine der folgenden Optionen:

  - Aktivieren Sie **ALL delegated admin roles**, um die Rollenzuordnungsregeln aller Authentifizierungsbereiche zu exportieren.

  - Klicken Sie auf **SELECTED delegated admin roles...**, und wählen Sie anschließend in der Liste **Available Roles** Rollen aus. Klicken Sie auf **Add**, wenn Sie nur diese Rollen exportieren möchten.

  Wählen Sie im Abschnitt **User Roles** eine der folgenden Optionen:

  - Wählen Sie **ALL user roles**, um alle lokalen Benutzerrollen zu exportieren.

  - Klicken Sie auf **SELECTED user roles...**, und wählen Sie anschließend in der Liste **Available Roles** Rollen aus. Klicken Sie auf **Add**, wenn Sie nur die ausgewählten Benutzerrollen exportieren möchten.

- Aktivieren Sie zum Exportieren von Ressourcenrichtlinien das Kontrollkästchen **Export Resource Policies**. Aktivieren Sie anschließend die Kontrollkästchen für die Typen von Ressourcenrichtlinien, die Sie exportieren möchten, beispielsweise Richtlinien für Zugriffssteuerung.

- Aktivieren Sie zum Exportieren aller lokaler Benutzerkonten das Kontrollkästchen **Export Local User Accounts**. Als Nächstes wählen Sie eine der folgenden Optionen:

  - Wählen Sie **From ALL local auth servers**, um alle lokalen Benutzerkonten von allen lokalen Authentifizierungsservern zu exportieren.

  - Aktivieren Sie **From SELECTED local auth servers...**, wählen Sie in der Liste **Available Servers** Authentifizierungsserver aus, und klicken Sie zum Exportieren der lokalen Benutzer dieser lokalen Authentifizierungsserver auf **Add**.

- Aktivieren Sie das Kontrollkästchen **Log/Monitoring**, um Protokoll-/Überwachungsdaten zu exportieren.

  - Aktivieren Sie **SNMP**, um SNMP-Daten einschließlich der Trap-Einstellungen und -Grenzwerte zu exportieren.

4. Klicken Sie auf **Export...**, um die Informationen in einer XML-Datei zu speichern.

XML-Konfigurationsdaten importieren

So importieren Sie XML-Konfigurationsdaten:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > XML Import/Export > Import** aus.

2. Klicken Sie unter **Schema Files** auf den Link, um die XML-Schemadateien (.xsd) herunterzuladen, die die IVE-Objekte beschreiben (optional). Weitere Informationen zu Schemadateien finden Sie „Herunterladen von Schemadateien“ auf Seite 141.

3. Navigieren Sie zur XML-Datendatei, die Sie importieren möchten, und wählen Sie sie aus. Wenn Sie nur eine Teilkonfiguration importieren möchten, importieren Sie eine gültige XML-Fragmentdatei.

4. Wählen Sie den **Import Mode**:

   - **Full Import** (Hinzufügen, Aktualisieren und Löschen) – Fügt neue Datenelemente aus der importierten XML-Datei zur IVE-Konfiguration hinzu, aktualisiert bestehende Elemente, deren Werte in der importierten XML-Datei geändert werden, und löscht bestehende Elemente, die in der importierten XML-Datei nicht definiert sind.

HINWEIS: VORSICHT. Die Verwendung des Modus **Full Import** ist nicht ganz ungefährlich. Bei unachtsamer Vorgehensweise kann die IVE-Konfiguration versehentlich ganz oder teilweise gelöscht werden. Im Modus **Full Import** ersetzt das IVE die Konfiguration der IVE-Appliance mit dem Inhalt der Instanzdatei. Alle nicht definierten Elemente der Instanzdatei werden aus der IVE-Appliance gelöscht.

   - **Standard Import** (Hinzufügen und Aktualisieren) – Fügt neue Datenelemente aus der importierten XML-Datei zur IVE-Konfiguration hinzu und aktualisiert bestehende Elemente, deren Werte in der importierten XML-Datei geändert werden. Keine Elemente werden gelöscht.

   - **Quick Import** (Hinzufügen) – Fügt neue Datenelemente aus der importierten XML-Datei zur IVE-Konfiguration hinzu. Änderungen bestehender Elemente werden ignoriert.

5. Klicken Sie auf **Import**. Die Seite Import XML Results mit Informationen über die importierten Netzwerkeinstellungen, Rollen und Ressourcenrichtlinien wird geöffnet.

   Treten Fehler in der XML auf, wird der Importvorgang angehalten und ein Rollback der Konfiguration zum vorherigen Status durchgeführt. Fehlermeldungen werden auf der Seite **Import XML Results** angezeigt.

6. Klicken Sie auf **OK**, um zur Seite **Import** zurückzukehren.

XML Import/Export – Gebrauchsfälle

Die folgenden Gebrauchsfälle veranschaulichen die Verwendung der Funktion **XML Import/Export**. Jeder Gebrauchsfall umfasst eine kurze Beschreibung und die Vorgehensweise zur Ausführung des Gebrauchsfalls. Dies ist eine gekürzte Darstellung der Gebrauchsfälle und umfasst nicht sämtliche Feinheiten und Details aller Vorgehensweisen. Die Gebrauchsfälle sind ausschließlich zur Veranschaulichung der Verwendung der Funktion **XML Import/Export** gedacht.

Gebrauchsfall: Einem IVE mehrere neue Benutzer hinzufügen

Sie haben dem Netzwerk soeben eine neue IVE-Appliance hinzugefügt und möchten dem System nun zweitausend Benutzer hinzufügen. Sie möchten die Benutzer der IVE-Webkonsole nicht einzeln hinzufügen, sondern einen Massenimport durchführen. Des Weiteren soll die Änderung der Kennwörter bei der ersten Anmeldung der Benutzer erzwungen werden. Sie können die Benutzerkonten exportieren, die relevante XML, die die Benutzer definiert, extrahieren, jedes Element nach Bedarf replizieren und sie anschließend ins IVE importieren.

In dieser Prozedur werden nur Beispiele für Benutzer 1, Benutzer 2 und Benutzer 2000 angezeigt. Von allen weiteren Benutzern wird angenommen, dass sie in der Importdatei enthalten sind. Die Kennwörter werden als durchnummerierte Versionen des Wortes „password“ festgelegt, z. B. *password1*, *password2* usw. Alle Benutzer in diesem Beispiel werden demselben Authentifizierungsserver zugewiesen, obwohl Sie jede Kombination der im System gültigen Authentifizierungsserver eingeben können.

So fügen Sie einem IVE mehrere neue Benutzer hinzu

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Export XML**.
2. Folgen Sie den Anweisungen in „XML-Konfigurationsdaten exportieren“ auf Seite 366, um lokale Benutzerkonten zu exportieren.
3. Speichern Sie die exportierte Datei unter *users.xml*.
4. Öffnen Sie die Datei *users.xml*.
5. Kopieren Sie das Benutzer-Containerelement, und fügen Sie es ein, bis Sie die erforderliche Anzahl an Benutzern hinzugefügt haben. Auch wenn das Beispiel nur drei neue Benutzer anzeigt, können Sie der Datei Hunderte neuer Benutzer hinzufügen.

6. Aktualisieren Sie die entsprechenden Daten in jedem Benutzer-Containerelement wie im folgenden Beispiel:

HINWEIS:

- Die ursprüngliche Formatierung des folgenden Beispiels wurde zur besseren Lesbarkeit geändert. Der tatsächliche XML-Code wird möglicherweise anders angezeigt.
- Sie müssen „PasswordFormat“ auf Plaintext einstellen, da das IVE andernfalls von der Standardeinstellung Encrypted ausgeht.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<IVE xmlns="http://xml.juniper.net/iveos/5.0R1/ive">
<AAA xmlns:aaa="http://xml.juniper.net/iveos/5.0R1/aaa">
    <aaa:Users>
        <aaa:User>
            <aaa:AuthServerName>System Local</aaa:AuthServerName>
            <aaa:Email>user1@company.com</aaa:Email>
            <aaa:FullName>User1</aaa:FullName>
            <aaa:LoginName>user1</aaa:LoginName>
            <aaa:Password PasswordFormat="Plaintext">password1
                </aaa:Password>
            <aaa:ChangePasswordAtNextLogin>true
                </aaa:ChangePasswordAtNextLogin>
        </aaa:User>

        <aaa:User>
            <aaa:AuthServerName>System Local</aaa:AuthServerName>
            <aaa:Email>user2@company.com</aaa:Email>
            <aaa:FullName>User2</aaa:FullName>
            <aaa:LoginName>user2</aaa:LoginName>
            <aaa:Password PasswordFormat="Plaintext">password2
                </aaa:Password>
            <aaa:ChangePasswordAtNextLogin>true
                </aaa:ChangePasswordAtNextLogin>
        </aaa:User>

        <aaa:User>
            <aaa:AuthServerName>System Local</aaa:AuthServerName>
            <aaa:Email>user2000@company.com</aaa:Email>
            <aaa:FullName>User 2000</aaa:FullName>
            <aaa:LoginName>user2000</aaa:LoginName>
            <aaa:Password PasswordFormat="Plaintext">password2000
                </aaa:Password>
            <aaa:ChangePasswordAtNextLogin>true
                </aaa:ChangePasswordAtNextLogin>
        </aaa:User>
    </aaa:Users>
</AAA>
<SYS xmlns:sys="http://xml.juniper.net/iveos/5.0R1/sys"/>
</IVE>
```

7. Speichern Sie die Datei *users.xml*.

8. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Import XML**.

9. Wählen Sie entweder **Standard Import** oder **Quick Import** aus.

10. Importieren Sie die Datei wie in „XML-Konfigurationsdaten importieren“ auf Seite 369 beschrieben.

Gebrauchsfall: Richtlinien aktualisieren

Sie möchten alle ActiveX-Richtlinien für das Neuschreiben von *RewriteURLResponseForDynamicStaticHTML* in eine andere Aktion ändern, möchten jedoch nicht jede Richtlinie einzeln in die Webkonsole eingeben. Stattdessen können Sie eine Instanzdatei exportieren, Änderungen vornehmen und anschließend die Datei zurück ins IVE importieren.

So aktualisieren Sie Richtlinien in einem IVE

Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Export XML**.

1. Folgen Sie den Anweisungen in „XML-Konfigurationsdaten exportieren“ auf Seite 366, um lokale Benutzerkonten zu exportieren.

2. Speichern Sie die exportierte Datei unter *policy.xml*.

3. Öffnen Sie die exportierte Datei.

4. Öffnen Sie die Schemadatei *policy.xsd* im System, indem Sie entweder einen Text-Editor oder einen XML-Editor verwenden. Suchen Sie in der Schemadatei nach dem Aktionswert *RewriteURLResponseForDynamicStaticHTML*. Die Schemadefinition für **ActiveXActionType** beinhaltet den aktuellen Aktionswert der Richtlinie sowie weitere mögliche Werte. Siehe folgendes Beispiel:

```
<xs:simpleType name="ActiveXActionType">
        <xs:restriction base="xs:token">
            <xs:enumeration value="RewriteURLResponseForStaticHTML"/>
            <xs:enumeration
                value="RewriteURLResponseForDynamicStaticHTML"/>
            <xs:enumeration value="RewriteURLForStaticHTML"/>
            <xs:enumeration value="RewriteURLForDynamicStaticHTML"/>
            <xs:enumeration value="RewriteHostForStaticHTML"/>
            <xs:enumeration value="RewriteHostForDynamicStaticHTML"/>
            <xs:enumeration value="DoNotRewrite"/>
        </xs:restriction>
    </xs:simpleType>
```

5. Suchen Sie in der exportierten Datei *policy.xml* *RewriteURLResponseForDynamicStaticHTML*, und ersetzen Sie es durch den Aktionswert *RewriteURLForDynamicStaticHTML*.

HINWEIS: Das folgende Beispiel zeigt nur ein Fragment der tatsächlichen Datei policy.xml. Die ursprüngliche Formatierung wurde ebenfalls zur besseren Lesbarkeit geändert. Der tatsächliche XML-Code wird möglicherweise anders angezeigt.

```
<!– DO NOT MODIFY OR DELETE THE FIRST THREE LINES –>
<IVE xmlns="http://xml.juniper.net/iveos/5.0R1/ive">
<AAA xmlns:aaa="http://xml.juniper.net/iveos/5.0R1/aaa">
<aaa:ResourcePolicyList>
<aaa:WebActiveXRewritingPolicyList>
    <aaa:ActiveXRewritingPolicy>
        <aaa:ParameterList>
            <aaa:Parameter>
                <aaa:Name>URL</aaa:Name>
                <!– Change the following data –>
                <aaa:Action>RewriteURLResponseForDynamicStaticHTML
                    </aaa:Action>
            </aaa:Parameter>
        </aaa:ParameterList>
        <aaa:Description>OrgPlus Orgviewer</aaa:Description>
        <aaa:ClassID>DCB98BE9-88EE-4AD0-9790-2B169E8D5BBB
            </aaa:ClassID>
    </aaa:ActiveXRewritingPolicy>
</aaa:ResourcePolicyList>
<!– DO NOT MODIFY OR DELETE THE LAST THREE LINES –>
</AAA>
<SYS xmlns:sys="http://xml.juniper.net/iveos/5.0R1/sys"/>
</IVE>
```

6. Speichern Sie die Datei *policy.xml*.

7. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Import XML**.

8. Wählen Sie **Standard Import** aus. Durch Wählen dieses Importmodus aktualisieren Sie in der XML-Instanzdatei geänderte Daten im IVE.

9. Importieren Sie die Datei wie in „XML-Konfigurationsdaten importieren“ auf Seite 369 beschrieben.

Gebrauchsfall: Benutzer aus einem IVE löschen

Jeden Monat werden Benutzer, die nicht länger im Unternehmen arbeiten, aus dem IVE entfernt. In einem großen Unternehmen müssen monatlich oft Dutzende oder sogar Hunderte von Benutzern gelöscht werden. Dies kann sehr zeitaufwendig sein, daher ist ein einfacher Arbeitsvorgang von Vorteil.

HINWEIS: VORSICHT. Die Verwendung des Modus **Full Import** ist nicht ganz ungefährlich. Bei unachtsamer Vorgehensweise kann die IVE-Konfiguration versehentlich ganz oder teilweise gelöscht werden. Im Modus **Full Import** ersetzt das IVE die Konfiguration der IVE-Appliance mit dem Inhalt der Instanzdatei. Alle nicht definierten Elemente der Instanzdatei werden aus der IVE-Appliance gelöscht.

So löschen Sie Benutzer aus einem IVE

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Export XML**.

2. Folgen Sie den Anweisungen in „XML-Konfigurationsdaten exportieren“ auf Seite 366, um lokale Benutzerkonten zu exportieren.

3. Speichern Sie die exportierte Datei unter *remusers.xml*.

4. Öffnen Sie die Datei *remusers.xml*.

5. Haben Sie eine Liste von zu löschenden Benutzern, durchsuchen Sie die Datei nach jedem Benutzernamen, und entfernen Sie anschließend das gesamte Benutzer-Containerelement, das den Benutzernamen enthält. Im folgenden Beispiel werden der Benutzercontainer und seine untergeordneten Elemente angezeigt:

```
<aaa:User>
    <aaa:AuthServerName>System Local</aaa:AuthServerName>
        <aaa:Email>deleteuser@company.com</aaa:Email>
        <aaa:FullName>DeleteUser</aaa:FullName>
        <aaa:LoginName>deleteuser</aaa:LoginName>
        <aaa:Password
            PasswordFormat="Encrypted">oU63QjnZCgABAAAA91aVaD
        </aaa:Password>
        <aaa:ChangePasswordAtNextLogin>false
            </aaa:ChangePasswordAtNextLogin>
</aaa:User>
```

HINWEIS: Versuchen Sie niemals, ein Kennwort manuell in der XML-Datei zu verschlüsseln. Das IVE verweigert alle derartigen Versuche. Verwenden Sie das Klartextkennwortformat (PasswordFormat), und geben Sie beim Ändern von Kennwörtern über die XML-Datei ein Kennwort in Klartext ein.

6. Speichern Sie die Datei *remusers.xml*.

7. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Import XML**.

8. Wählen Sie **Full Import** aus. Durch Wählen dieses Importmodus ersetzen Sie alle Benutzerdaten im IVE mit den Benutzerdaten aus der XML-Instanzdatei.

9. Importieren Sie die Datei wie in „XML-Konfigurationsdaten importieren“ auf Seite 369 beschrieben.

Gebrauchsfall: XML Import/Export in einer Clusterumgebung verwenden

Sie können die Funktion XML Import/Export in einer Clusterumgebung verwenden. Sie müssen jedoch gewisse Regeln und eine bestimmte Vorgehensweise einhalten, um den Vorgang erfolgreich abzuschließen.

- Die zu importierende XML-Instanz muss denselben Knotensatz wie der ursprüngliche Cluster enthalten. Die Signatur, die zur Synchronisation des Clusters bei reaktivierten Knoten verwendet wird, wird von der IP-Adresse des Clusterknotens abgeleitet. Die verbleibenden Knoten können dem Cluster also nicht wieder beitreten, wenn die importierte Konfiguration eine andere Signatur enthält.

- Ändern Sie nicht den Knotennamen, die IP-Adresse oder die IP-Netzmaske in der Instanzdatei.

- Verwenden Sie nicht den Modus Full Import. Verwenden Sie ausschließlich den Modus Standard Import.

- Ändern Sie in der Instanzdatei keine Netzwerkeinstellungen, die bewirken, dass der primäre Knoten nicht erreichbar ist. Ändern Sie beispielsweise nicht die Standardgatewaykonfiguration für einen Multisite-Cluster.

- Beim Import überschreibt die Instanzdatei die knotenspezifischen Netzwerkeinstellungen der Clusterkonfiguration für die verbleibenden Knoten. Achten Sie beim Ändern dieser knotenspezifischen Netzwerkeinstellungen darauf, dass die verbleibenden Knoten erreichbar bleiben.

- Ändern Sie keine bestehenden virtuellen Porteinstellungen, oder fügen Sie der Instanzdatei keine neuen virtuellen Porteinstellungen hinzu.

So verwenden Sie XML Import/Export in einer Clusterumgebung

1. Deaktivieren Sie weitere Clusterknoten Ihres primären IVE auf der Seite **System > Clustering > Status**.

2. Exportieren Sie die XML-Instanz aus **Maintenance > Import/Export > Export XML**.

3. Ändern Sie die XML-Instanz gemäß der Anleitung in „Erstellen und Ändern von XML-Instanzen“ auf Seite 133.

4. Importieren Sie die XML-Instanz gemäß der Anleitung in „Importieren und Exportieren von XML-Konfigurationsdateien“ auf Seite 130.

5. Aktivieren Sie die Clusterknoten in der Webkonsole auf der Seite **System > Clustering > Status**.

Konfigurieren der Seite „Archiving“

Die Seite **Archiving** enthält die folgende Registerkarte:

- „Registerkarte „FTP Server““ auf Seite 376 – Auf dieser Registerkarte können Sie das Archivieren von Systemdaten auf einem externen FTP- oder SCP-Server planen.

Registerkarte „FTP Server“

Auf dieser Registerkarte können Sie das Archivieren von Systemdaten auf einem externen FTP- oder SCP-Server planen. Die Beschreibung dazu finden Sie in „Archivieren von IVE-Konfigurationsdateien“ auf Seite 129.

Planen der Archivierung von Systemdaten auf einem externen FTP- oder SCP-Server

So legen Sie Archivierungsparameter fest:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Archiving > FTP Archiving**.
2. Geben Sie unter **Archive Settings** den Zielserver, ein Verzeichnis und Ihre FTP-Anmeldeinformationen für diesen Server an. Schließen Sie keine Laufwerksangabe für das Zielverzeichnis ein, beispielsweise: juniper/log.
   - Wir empfehlen, bei UNIX-Computern einen vollständigen Pfad anzugeben, auch wenn Sie abhängig vom Basisverzeichnis des Benutzers einen absoluten oder relativen Pfad angeben können.
   - Bei Windows-Computern geben Sie einen Pfad an, der relativ zum Verzeichnis ftproot ist. Wir empfehlen die Verwendung eines vollständigen Pfads zum Verzeichnis.
3. Geben Sie unter **Method** SCP oder FTP an. SCP ist die Standardmethode.
4. Geben Sie unter **Archive Schedule** mindestens eine der folgenden Komponenten für die Archivierung an, indem Sie das entsprechende Kontrollkästchen aktivieren:
   - **Archive events log** (Weitere Informationen finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 126.)
   - **Archive user access log** (Weitere Informationen finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 126.)
   - **Archive admin access log** (Weitere Informationen finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 126.)
   - **Archive NC packet log** (Weitere Informationen finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 126.)

- **Archive system configuration** (Weitere Informationen finden Sie unter „Registerkarte „Configuration““ auf Seite 364.)
- **Archive user accounts** (Weitere Informationen finden Sie unter „Registerkarte „User Accounts““ auf Seite 365.)

5. Klicken Sie auf **Save Changes**.

Konfigurieren der Seite „Troubleshooting“

Die Seite **Troubleshooting** enthält die folgenden Registerkarten:

- „„User Sessions“-Registerkarten“ auf Seite 378 – Auf dieser Registerkarte können Sie Optionen für Benutzersitzungen angeben, um eine Benutzersitzung zu simulieren und eine Richtlinienverfolgungsdatei aufzuzeichnen.
- „Registerkarte „Session Recording““ auf Seite 381 – Zeichnen Sie mithilfe dieser Registerkarte eine Ablaufverfolgungsdatei zu Debuggingzwecken auf.
- „Registerkarte „System Snapshot““ auf Seite 382 – Erstellen Sie auf dieser Registerkarte einen Snapshot des IVE-Systemstatus.
- „Registerkarte „TCP Dump““ auf Seite 382 – Auf dieser Registerkarte können Sie Sniffing von Netzwerkpaketheadern durchführen.
- „Registerkarte „Commands““ auf Seite 383 – Auf dieser Registerkarte können Sie einen ARP-, Ping-, Traceroute- oder Nslookup-Befehl ausführen.
- „Registerkarte „Remote Debugging““ auf Seite 384 – Auf dieser Registerkarte können Sie Remotedebugging für Juniper Networks-Support aktivieren.
- „Registerkarte „Debug Log““ auf Seite 385 – Auf dieser Registerkarte können Sie das Debugprotokoll aktivieren.

„User Sessions“-Registerkarten

Registerkarte „Policy Tracing“

Mit dieser Registerkarte können Sie Probleme beheben, indem Sie die Ereignisse bei der Anmeldung eines Benutzers an einem Bereich verfolgen.

Aufzeichnen einer Richtlinienverfolgungsdatei

Verwenden Sie diese Registerkarte, wenn die Benutzer Probleme beim Zugreifen auf Funktionen feststellen, die sie normalerweise im Rahmen ihrer jeweiligen Rollen verwenden können. Mithilfe der in der Richtlinienverfolgungsdatei protokollierten Ereignisse können Sie diese Probleme diagnostizieren. Beachten Sie, dass Benutzerzugriffsprotokolle nur für die unter **Events to Log** aktivierten Richtlinien protokolliert werden.

So erstellen Sie eine Richtlinienverfolgungsdatei:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > User Sessions > Policy Tracing**.
2. Geben Sie im Feld **User** den IVE-Benutzernamen des Benutzers ein, den Sie verfolgen möchten. Sie können anstelle eines Benutzernamens auch einen Platzhalter (*) verwenden. Wenn sich die Benutzer beispielsweise an einem anonymen Server anmelden, kann es ratsam sein, den Platzhalter (*) zu verwenden, da Sie den internen Benutzernamen, der dem Benutzer vom IVE zugewiesen wird, nicht kennen.

3. Wählen Sie im Feld **Realm** den Bereich des Benutzers aus. Beachten Sie, dass auf dem IVE kein Bereich ausgewählt werden kann, der einem anonymen Authentifizierungsserver zugeordnet ist.

4. Aktivieren Sie unter **Events to log** die Ereignistypen, die in der Protokolldatei für die Richtlinienverfolgung erfasst werden sollen.

5. Klicken Sie auf **Start Recording**. Bitten Sie den Benutzer nach dem Beginn der Aufzeichnung, sich am IVE anzumelden.

6. Klicken Sie zum Anzeigen der Protokolleinträge auf **View Log**.

7. Klicken Sie auf **Stop Recording**, wenn Sie genügend Informationen erfasst haben.

8. Überprüfen Sie die Meldungen in der Protokolldatei, um den Grund für das abweichende Verhalten zu finden. Wenn Sie das Problem nicht erkennen und beheben können, klicken Sie auf **Save Log As**, und speichern Sie eine Kopie der Protokolldatei im Netzwerk. Senden Sie die Datei anschließend zur Überprüfung an den Juniper Networks-Support.

9. Klicken Sie auf **Clear Log**, um den Inhalt der Protokolldatei zu löschen, oder auf **Delete Trace**, um den Inhalt der Protokolldatei zu löschen und die Standardeinträge aus den Feldern für Benutzername und Bereich zu entfernen.

Registerkarte „Simulation“

Mit dieser Registerkarte können Sie Probleme lösen, indem Sie die Ereignisse simulieren, die das Problem verursachen.

Simulieren einer Benutzersitzung

So simulieren Sie eine Benutzersitzung:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > User Sessions > Simulation**.

2. Geben Sie im Feld **Query Name** einen Namen für die Abfrage ein.

3. Geben Sie im Feld **Username** den Benutzernamen des IVE-Benutzers ein, für den Sie eine Simulation ausführen möchten. Sie können anstelle eines Benutzernamens auch einen Platzhalter (*) verwenden. Wenn sich die Benutzer beispielsweise an einem anonymen Server anmelden, kann es ratsam sein, den Platzhalter (*) zu verwenden, da Sie den internen Benutzernamen, der dem Benutzer vom IVE zugewiesen wird, nicht kennen.

4. Wählen Sie im Dropdownmenü **Realm** den Bereich des IVE-Benutzers aus, für den Sie eine Simulation ausführen möchten.

5. Wenn Sie festlegen möchten, ob das IVE auf die Sitzung eines Benutzers eine bestimmte Art von Ressourcenrichtlinie anwendet, geben Sie die zu simulierende Ressource ins Feld **Resource** ein, und wählen Sie in der Dropdownliste **Resource** einen Richtlinientyp aus. Gehen Sie anschließend folgendermaßen vor:

   - Wenn Sie ermitteln möchten, ob sich ein Benutzer erfolgreich beim IVE anmelden kann, aktivieren Sie das Kontrollkästchen **Pre-Authentication**.
   - Um zu ermitteln, ob einem Benutzer eine bestimmte Rolle zugeordnet werden kann, aktivieren Sie das Kontrollkästchen **Role Mapping**. Beachten Sie, dass mit dieser Option gesteuert wird, ob die Ergebnisse der Rollenzuordnung im Simulationsprotokoll aufgezeichnet werden. Es wird jedoch nicht gesteuert, ob das IVE Rollenzuordnungsregeln ausführt. Das IVE führt grundsätzlich Rollenzuordnungsregeln aus, unabhängig davon, ob Sie dieses Kontrollkästchen aktivieren oder deaktivieren.
   - Legen Sie die zu protokollierenden Richtlinientypen mithilfe der Kontrollkästchen im Abschnitt **Events to Log** fest.

   Wenn Sie z. B. testen möchten, ob ein Benutzer auf die Yahoo-Website zugreifen kann, geben Sie im Feld **Resource** die Zeichenfolge http://www.yahoo.com ein. Wählen Sie dann in der Dropdownliste den Eintrag **Web** aus, und aktivieren Sie im Abschnitt **Events to Log** das Kontrollkästchen **Access**.

6. Verwenden Sie im Abschnitt **Variables** eine Kombination aus Text und Variablen, um einen benutzerdefinierten Ausdruck zu erstellen, der genau dieselben Werte wie in der tatsächlichen Sitzung des Benutzers widerspiegelt, bei dem ein Problem aufgetreten ist. Wenn Sie beispielsweise eine Sitzung erstellen möchten, in der sich der Benutzer um 6:00 Uhr beim IVE anmeldet, geben Sie im Feld **Variables** Folgendes ein: “time = 6:00 AM”. Umfassende Anweisungen zum Erstellen eines benutzerdefinierten Ausdrucks finden Sie unter „Schreiben benutzerdefinierter Ausdrücke“ auf Seite 397. Sie können auch die Syntax für eine bestimmte Variable anzeigen, indem Sie in **Variables Dictionary** auf den Pfeil neben der entsprechenden Variable klicken.

HINWEIS: Wenn Sie keinen benutzerdefinierten Ausdruck erstellen können, der die IP-Adresse des virtuellen Benutzers umfasst, verwendet das IVE stattdessen Ihre aktuelle IP-Adresse. Darüber hinaus sollten Sie beachten, dass das IVE bei Verwendung der Rollenvariable zum Angeben der Rolle des virtuellen Benutzers (z. B. role = ”Users”) die Ergebnisse der Rollenzuordnungsregeln ignoriert und den virtuellen Benutzer den von Ihnen angegebenen Rollen zuweist.

7. Wählen Sie eine der folgenden Optionen aus:

   - **Run Simulation** – Führt die angegebene Simulation aus und erstellt eine Bildschirmprotokolldatei.
   - **Save Query** – Speichert die Abfrage.
   - **Save Query and Run Simulation** – Führt die angegebene Simulation aus und speichert sie für eine spätere Verwendung.

8. Wählen Sie nach dem Ausführen der Simulation die Option **Save Log As** aus, um die Ergebnisse der Simulation in einer Textdatei zu speichern.

Registerkarte „Session Recording“

Verwenden Sie diese Registerkarte zum Aufzeichnen einer Ablaufverfolgungsdatei, die alle Aktionen eines Benutzers aufzeichnet, wenn dieser auf eine mit dem IVE nicht korrekt anzeigbare Webseite zugreift oder eine Verbindung zu einer Client-Server-Anwendung herstellt, die über das IVE nicht wie erwartet funktioniert.

Aufzeichnen einer Ablaufverfolgungsdatei zu Debuggingzwecken

So zeichnen Sie eine Ablaufverfolgungsdatei auf:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Session Recording** aus.

2. Geben Sie den Namen des Benutzers ein, dessen Sitzung aufgezeichnet werden soll.

3. Aktivieren Sie das Kontrollkästchen **Web (DSRecord)** zur Aufzeichnung der Websitzung des Benutzers. Aktivieren Sie das Kontrollkästchen **Ignore browser cache**, wenn zwischengespeicherte Kopien der Problem-Website ignoriert werden sollen – diese werden vom IVE ansonsten nicht als Teil der Ablaufsverfolgungsdatei aufgezeichnet (optional).

4. Aktivieren Sie das Kontrollkästchen **Client/Server (JCP + NCP)** zum Aufzeichnen von Java Communication Protocol- und Network Communication Protocol-Client-Server-Anwendungssitzungen (optional).

5. Klicken Sie auf **Start Recording**. Das IVE meldet den Benutzer ab.

6. Weisen Sie den Benutzer an, sich erneut anzumelden und die Problem-Website aufzurufen oder über das IVE eine Verbindung zur Client-Server-Anwendung herzustellen.

7. Klicken Sie auf **Stop Recording**.

8. Laden Sie die Ablaufverfolgungsdatei(en) aus dem Abschnitt **Current Trace File** herunter:

   a. Klicken Sie auf den Link **DSRecord Log**, um die Web-Ablaufverfolgungsdatei herunterzuladen.

   b. Klicken Sie auf den Link **JCP** oder **NCP Client-Side Log**, um die Ablaufverfolgungsdatei für die Client-Server-Anwendung herunterzuladen.

9. Senden Sie die Datei(en) zur Überprüfung per E-Mail an den Juniper Networks-Support.

10. Klicken Sie auf die Schaltfläche **Delete**, um die soeben erstellten Ablaufverfolgungsdatei(en) zu entfernen (optional).

Registerkarte „System Snapshot“

Erstellen Sie auf dieser Registerkarte einen Snapshot des IVE-Systemstatus. Weitere Informationen über Snapshots finden Sie unter „Erstellen von Snapshots des IVE-Systemstatus“ auf Seite 145.

Erstellen eines Snapshots des IVE-Systemstatus.

So erstellen Sie einen Snapshot des IVE-Systemstatus:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > System Snapshot**.
2. Aktivieren Sie das Kontrollkästchen **Include system config**, um Informationen zur Systemkonfiguration in den Snapshot einzuschließen (optional).
3. Aktivieren Sie das Kontrollkästchen **Include debug log**, um die mithilfe der Registerkarte **Debug Log** erstellte Protokolldatei in den Systemschnappschuss einzuschließen. Weitere Informationen finden Sie unter „Registerkarte „Debug Log““ auf Seite 385.
4. Klicken Sie auf **Take Snapshot**.
5. Wenn das IVE das Erstellen des Snapshots beendet hat, klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen.
6. Senden Sie die Datei zur Überprüfung per E-Mail an den Juniper Networks-Support.
7. Klicken Sie abschließend zum Löschen des Schnappschusses auf **Delete**.

HINWEIS: Ein Systemsnapshot kann auch von der seriellen Konsole erstellt werden. Diese Methode ist von Vorteil, wenn Sie die Webkonsole nicht erreichen können und die Systemkonfiguration speichern müssen. Weitere Informationen finden Sie unter „Durchführen gängiger Wiederherstellungsvorgänge“ auf Seite 395.

Registerkarte „TCP Dump“

Auf dieser Registerkarte können Sie Sniffing von Netzwerkpaketheadern durchführen und die Ergebnisse in einer verschlüsselten „Dumpdatei“ bzw. Sicherungsdatei speichern. Diese können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den Juniper Networks-Support senden. Weitere Informationen zur Verwendung von „TCP Dump“ finden Sie unter „Erstellen von TCP-Dumpdateien“ auf Seite 145.

Sniffing von Netzwerkpaketheadern

So führen Sie das Sniffing von Netzwerkpaketheadern aus:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > TCP Dump**.
2. Wählen Sie den IVE-Port aus, an dem Sniffing von Netzwerkpaketheadern durchgeführt werden soll.

3. Deaktivieren Sie den **Promiscuous mode**, so dass Sniffing nur für Pakete durchgeführt wird, die für das IVE bestimmt sind.

4. Erstellen Sie einen benutzerdefinierten Filter mithilfe von TCPDump-Filterausdrücken (optional). Diese Option bietet die Möglichkeit zum Filtern der gesnifften Netzwerkpakete, um sicherzustellen, dass die dabei erzeugte Dumpdatei nur die benötigten Informationen enthält. Tabelle 21 unten enthält Beispiele hierzu.

5. Klicken Sie auf **Start Sniffing**.

6. Klicken Sie auf **Stop Sniffing**, um das Sniffing zu beenden und eine verschlüsselte Datei zu erstellen.

7. Klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen.

8. Senden Sie die Datei zur Überprüfung per E-Mail an den Juniper Networks-Support.

Tabelle 21: Beispiele von TCPDump-Filterausdrücken

Beispiel	Ergebnis
tcp port 80	Snifft Pakete auf TCP-Port 80.
port 80	Snifft Pakete auf TCP- oder UDP-Port 80.
ip	Snifft das IP-Protokoll.
tcp	Snifft das TCP-Protokoll.
dst #.#.#.#	Snifft die angegebene IP-Zieladresse (#.#.#.# ist eine gültige IP-Adresse).
src #.#.#.#	Snifft die angegebene IP-Quelladresse (#.#.#.# ist eine gültige IP-Adresse).
port 80 or port 443	Snifft an Port 80 oder Port 443.
src #.#.#.# and dst #.#.#.#	Snifft die IP-Ziel- und IP-Quelladresse oder angegebenen Hosts (#.#.#.# ist eine gültige IP-Adresse).
tcp port 80 or port 443 and dst #.#.#.# and src #.#.#.#	Dieses Beispiel zeigt, wie Sie mehrere Parameter angeben, um einen Filter zu erstellen, der an TCP-Port 80 oder an TCP- oder UDP-Port 443 und am Ziel- und Quellport snifft (#.#.#.# ist eine gültige IP-Adresse).
Auf der folgenden Website finden Sie Informationen über TCPDump-Filterausdrücke: http://www.tcpdump.org/tcpdump_man.html	

Registerkarte „Commands“

Auf dieser Registerkarte können Sie UNIX-Befehle ausführen, um die IVE-Netzwerkverbindung zu testen.

Ausführen eines ARP-, Ping- oder Traceroute-Befehls

So führen Sie einen UNIX-Befehl aus, um die IVE-Netzwerkverbindung zu testen

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Commands** aus.
2. Wählen Sie in der Liste **Command** den Befehl aus, der ausgeführt werden soll.
3. Geben Sie im Feld **Target Server** die IP-Adresse des Zielservers ein.
4. Geben Sie weitere Argumente oder Optionen ein.
5. Klicken Sie zur Ausführung des Befehls auf **OK**.

Ausführen eines NSLookup-Befehls

So führen Sie einen NSLookup-Befehl zum Testen der Namensserververbindung aus:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Commands** aus.
2. Wählen Sie in der Liste **Command** den NSLookup-Befehl aus.
3. Wählen Sie im Dropdownmenü die Option **Query Type** aus.
4. Geben Sie die Abfrage ein. Hierbei kann es sich je nach ausgewähltem Abfragetyp um einen Hostnamen, eine IP-Adresse oder andere Informationen handeln.
5. Geben Sie den DNS-Servernamen oder die IP-Adresse ein.
6. Geben Sie weitere Optionen ein.
7. Klicken Sie zur Ausführung des Befehls auf **OK**.

Registerkarte „Remote Debugging“

Auf dieser Registerkarte können Sie es dem Team vom Juniper Networks-Support ermöglichen, auf Ihrem Produktions-IVE Debuggingtools auszuführen.

Aktivieren des Remote-Debbuggings für den Juniper Networks-Support

So aktivieren Sie Remotedebugging:

1. Wenden Sie sich an den Juniper Networks-Support, um die Bedingungen für eine Remotedebuggingsitzung einzurichten.
2. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Remote Debugging**.
3. Geben Sie den Debuggingcode ein, der vom Juniper Networks-Support zur Verfügung gestellt wurde.
4. Geben Sie den Hostnamen ein, der vom Juniper Networks-Support zur Verfügung gestellt wurde.

5. Klicken Sie auf **Enable Debugging**, sodass das Team vom Juniper Networks-Support auf das IVE zugreifen kann.

6. Teilen Sie dem Juniper Networks-Support mit, dass auf Ihr IVE zugegriffen werden kann.

7. Klicken Sie auf **Disable Debugging**, wenn Ihnen der Juniper Networks-Support mitteilt, dass die Remotedebuggingsitzung beendet ist.

Registerkarte „Debug Log“

Verwenden Sie die Registerkarte **Debug Log**, um ein Debugprotokoll zu erstellen, das Sie an den Juniper Networks-Support senden können.

Aktivieren des Debugprotokolls

So aktivieren Sie das Debugprotokoll:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Debug Log**.

2. Aktivieren Sie das Kontrollkästchen **Debug Logging On**.

3. Geben Sie die Protokollgröße, die Detailebene und den vom Juniper Networks-Support angegebenen Ereigniscode ein.

4. Wählen Sie die Registerkarte **Maintenance > Troubleshooting > System Snapshot**.

5. Aktivieren Sie das Kontrollkästchen **Include debug log**.

6. Klicken Sie auf **Take snapshot**, um eine Datei mit dem Debugprotokoll zu erstellen.

7. Klicken Sie auf **Download**.

8. Fügen Sie die Schnappschussdatei einer E-Mail hinzu, und senden Sie diese an den Juniper Networks-Support.

Teil 4
Zusatzinformationen

Dieser Abschnitt enthält zusätzliche Informationen zur Konfiguration des IVE.

Inhalt

- „Verwenden der seriellen Konsole der IVE-Appliance“ auf Seite 389
- „Schreiben benutzerdefinierter Ausdrücke“ auf Seite 397
- „Installation von clientseitigen Anwendungen“ auf Seite 411
- „Konfigurieren der Zugriffsverwaltungsbeschränkungen“ auf Seite 417
- „Benutzerfehlermeldungen“ auf Seite 427

Anhang A

Verwenden der seriellen Konsole der IVE-Appliance

In diesem Abschnitt werden das Herstellen einer Verbindung mit der seriellen Konsole einer IVE-Appliance und die Ausführung von unterstützten Aufgaben beschrieben. Folgende Themen werden behandelt:

- „Herstellen einer Verbindung mit der seriellen Konsole der IVE-Appliance“ auf Seite 389
- „Rollback zu einem vorherigen Systemzustand“ auf Seite 390
- „Zurücksetzen einer IVE-Appliance auf die Werkseinstellungen“ auf Seite 392
- „Durchführen gängiger Wiederherstellungsvorgänge“ auf Seite 395

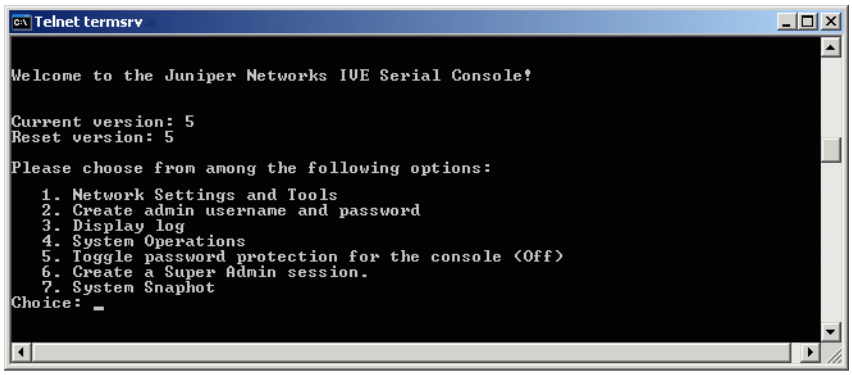
Herstellen einer Verbindung mit der seriellen Konsole der IVE-Appliance

Um Aufgaben über die serielle Konsole einer IVE-Appliance durchzuführen, müssen Sie ein Konsolenterminal oder einen Laptop an das Gerät anschließen.

So stellen Sie eine Verbindung mit der seriellen Konsole der IVE-Appliance her:

1. Schließen Sie ein Nullmodem-Crossover-Kabel vom Konsolenterminal oder Laptop an der IVE-Appliance an. Dieses Kabel ist im Lieferumfang des Geräts enthalten. Verwenden Sie kein einfaches serielles Kabel.
2. Konfigurieren Sie die Terminalemulationssoftware (beispielsweise HyperTerminal) mit den folgenden Parametern für serielle Verbindungen:
   - 9600 Bit pro Sekunde
   - 8 Bit, keine Parität (8N1)
   - 1 Stopp-Bit
   - Keine Flusskontrolle
3. Drücken Sie die **Eingabetaste**, bis die serielle Konsole des IVE angezeigt wird.

Abbildung 35: IVE Serielle Konsole


Telnet termsrv
Welcome to the Juniper Networks IVE Serial Console!
Current version: 5
Reset version: 5
Please choose from among the following options:
1. Network Settings and Tools
2. Create admin username and password
3. Display log
4. System Operations
5. Toggle password protection for the console (Off)
6. Create a Super Admin session.
7. System Snaphot
Choice:

Rollback zu einem vorherigen Systemzustand

Die IVE-Appliance speichert die aktuellen Systemkonfigurationsinformationen und die des vorherigen Systemstatus.

HINWEIS: Ein Rollback zu einem vorherigen Systemzustand ist auch über die Webkonsole möglich. Dieser Vorgang ist unter „Installieren eines Juniper-Softwaredienstpakets“ auf Seite 360 beschrieben.

Rollback zu einem vorherigen Systemstatus über die Webkonsole

Wenn Sie das Serverpaket aktualisieren und Ihr Gerät in den vorherigen Zustand zurücksetzen möchten, empfehlen wir Ihnen, den folgenden Anweisungen zu folgen:

1. Navigieren Sie zu den zuvor gespeicherten System- und Benutzerkonfigurationsdateien, in denen die gewünschten Zustandsdaten gespeichert sind. (Dieser Schritt setzt voraus, dass Sie Ihre System- und Benutzerdaten durch den Export von Dateien über das Menu **Maintenance > Import/Export** der Webkonsole gesichert haben.)

2. Laden Sie das gewünschte IVE-Betriebssystem-Servicepaket von der Juniper-Supportsite herunter: http://www.juniper.net/support/

3. Importieren Sie das gewünschte IVE-Betriebssystem-Servicepaket über das Menü **Maintenance > System > Upgrade/Downgrade** der Webkonsole.

4. Importieren Sie die System- und Benutzerkonfigurationsdateien aus Schritt 1.

Rollback zu einem vorherigen Systemstatus über die serielle Konsole

Wenn Sie nicht auf die Webkonsole zugreifen können, stellen Sie eine Verbindung mit der seriellen Konsole her, um ein Rollback zum vorherigen Systemzustand durchzuführen.

HINWEIS: Wenn Sie bisher noch keine Aktualisierung des IVE-Betriebssystem-Servicepakets durchgeführt haben, gibt es keinen älteren Systemstatus, und die Option ist daher nicht verfügbar. Wenn Sie eine Aktualisierung des IVE-Betriebssystem-Servicepakets durchgeführt haben, gehen alle System- und Benutzerkonfigurationsdaten, die nach der Aktualisierung erstellt wurden, verloren. Dies vermeiden Sie, indem Sie die aktuellen Konfigurationsdateien vor dem Rollback des Systems exportieren und anschließend wieder importieren.

So führen Sie ein Rollback zum vorherigen IVE-Betriebssystem-Servicepaket durch:

1. Stellen Sie eine Verbindung mit der seriellen Konsole der IVE-Appliance her. Anweisungen hierfür finden Sie unter „Herstellen einer Verbindung mit der seriellen Konsole der IVE-Appliance“ auf Seite 389.

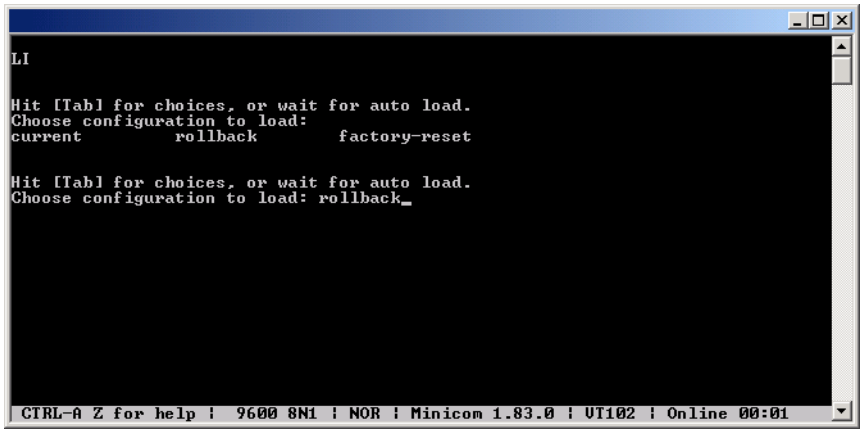
2. Melden Sie sich in einem Browserfenster an der Webkonsole an.

3. Wählen Sie **Maintenance > System > Platform** aus.

4. Klicken Sie auf **Reboot Now**, und wechseln Sie dann wieder zum Konsolenprogrammfenster zurück. Im Fenster werden Sie in einer Meldung informiert, dass das System neu gestartet wird.

5. Nach kurzer Zeit werden Sie aufgefordert, für die Auswahl von Optionen die **Tab-Taste** zu drücken. Drücken Sie die **Tabulator-Taste**. Wenn Sie gefragt werden, welche Konfiguration geladen werden soll, geben Sie rollback ein, und drücken Sie anschließend die **Eingabetaste**.

Abbildung 36: IVE Serielle Konsole


LI
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load:
current rollback factory-reset
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: rollback
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 1.83.0 | VT102 | Online 00:01

Nachdem Sie auf der Seite **Maintenance > System > Platform** auf **Reboot Now** geklickt haben, wird der Rollbackstatus des Servers auf dem Bildschirm angezeigt. Wenn der Vorgang abgeschossen ist, werden Sie zum Drücken der EINGABETASTE aufgefordert, um die Systemeinstellungen zu ändern. Dadurch kehren Sie zu den Optionen für das erste Setup zurück. Wenn Sie die Dateneingabe abgeschlossen haben, schließen Sie einfach das Programmfenster.

HINWEIS: Wenn Sie beim Auswählen länger als 5 Sekunden warten, wird automatisch die aktuelle Systemkonfiguration geladen. Sie müssen dann zur Webkonsole zurückkehren und auf **Reboot Now** klicken, um den Vorgang erneut zu starten. Wenn Sie bereits ein Systemrollback durchgeführt haben, ist die Rollbackoption erst wieder verfügbar, wenn Sie das IVE-Betriebssystem-Servicepaket erneut aktualisieren.

Zurücksetzen einer IVE-Appliance auf die Werkseinstellungen

In seltenen Fällen kann es erforderlich sein, die IVE-Appliance auf die Werkseinstellungen zurückzusetzen. Bevor Sie diese tief greifende Systemwiederherstellungsoption ausführen, sollten Sie sich an Juniper (http://www.juniper.net/support/) wenden. Vor dem Zurücksetzen auf die Werkseinstellungen sollten Sie nach Möglichkeit die aktuellen System- und Benutzerkonfigurationsdaten exportieren.

So setzen Sie das Gerät auf die Werkseinstellungen zurück:

1. Stellen Sie eine Verbindung mit der seriellen Konsole her. Anweisungen hierfür finden Sie unter „Herstellen einer Verbindung mit der seriellen Konsole der IVE-Appliance“ auf Seite 389.

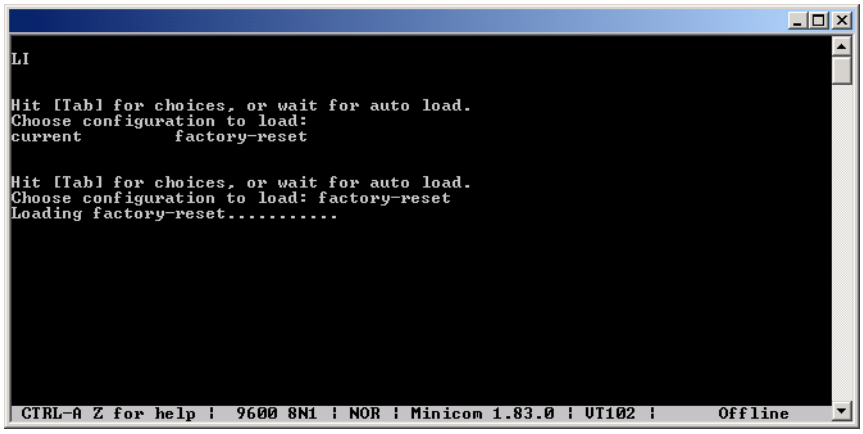
2. Melden Sie sich in einem Browserfenster an der Webkonsole an.

3. Wählen Sie **Maintenance > System > Platform** aus.

4. Klicken Sie auf **Reboot** IVE, und wechseln Sie dann wieder zum Fenster des Konsolenprogramms. Im Fenster werden Sie in einer Meldung informiert, dass das System neu gestartet wird.

5. Nach kurzer Zeit werden Sie aufgefordert, für die Auswahl von Optionen die **Tab-Taste** zu drücken. Drücken Sie die **Tab-Taste**. Wenn Sie gefragt werden, welche Konfiguration geladen werden soll, geben Sie factory-reset ein, und drücken Sie dann die **Eingabetaste**.

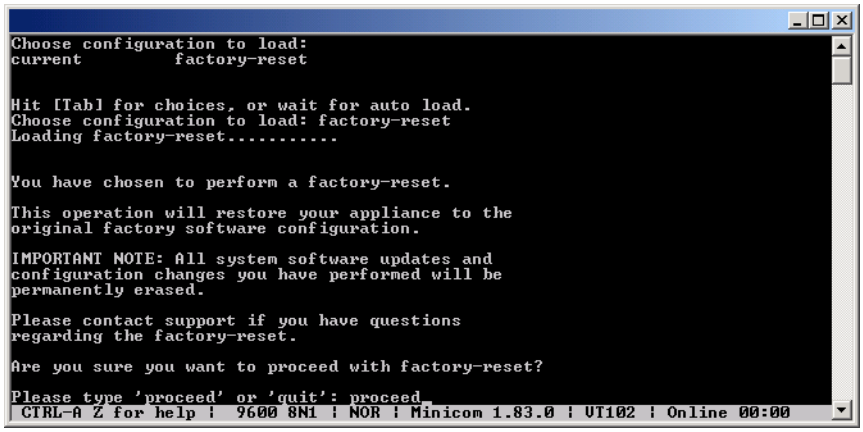
Abbildung 37: Serielle Konsole der IVE-Appliance nach dem Klicken auf „Reboot IVE“ auf der Seite „Maintenance > System > Platform“


LI
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load:
current factory-reset
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: factory-reset
Loading factory-reset.....
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 1.83.0 | VT102 | Offline

HINWEIS: Wenn Sie beim Auswählen länger als 5 Sekunden warten, wird automatisch die aktuelle Systemkonfiguration geladen. Sie müssen dann zurück in die Webkonsole wechseln und auf **Reboot Now** klicken, um den Vorgang erneut zu starten.

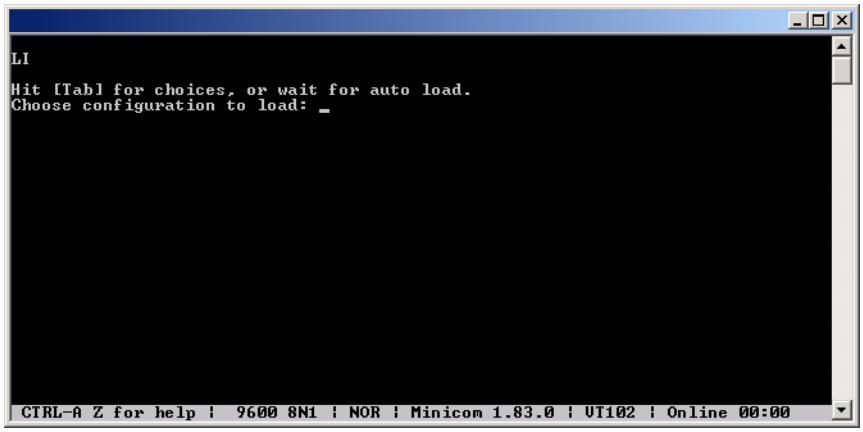
6. Wenn Sie aufgefordert werden, das Zurücksetzen auf die Werkseinstellungen zu bestätigen, geben Sie proceed ein, und drücken Sie dann die **Eingabetaste**.

Abbildung 38: Serielle Konsole der IVE-Appliance nach Auswahl der Option für die Wiederherstellung der Werkseinstellungen


Choose configuration to load:
current factory-reset
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: factory-reset
Loading factory-reset.....
You have chosen to perform a factory-reset.
This operation will restore your appliance to the
original factory software configuration.
IMPORTANT NOTE: All system software updates and
configuration changes you have performed will be
permanently erased.
Please contact support if you have questions
regarding the factory-reset.
Are you sure you want to proceed with factory-reset?
Please type 'proceed' or 'quit': proceed
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 1.83.0 | VT102 | Online 00:00

Das System beginnt mit dem Zurücksetzen des Geräts auf die Originaleinstellungen und gibt dabei mehrere Bildschirme mit Daten aus. Nach einigen Minuten werden Sie aufgefordert, für die Auswahl von Konfigurationsoptionen die **Tab-Taste** zu drücken.

Abbildung 39: Serielle Konsole der IVE-Appliance nach dem Zurücksetzen auf die Werkseinstellungen


LI
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load:
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 1.83.0 | VT102 | Online 00:00

7. Wenn Sie zum Drücken der **Tab-Taste** aufgefordert werden, gibt es folgende Möglichkeiten:

   - Warten Sie den automatischen Start der Standardoption ab (current), oder
   - drücken Sie die Tabstopptaste, geben Sie current ein, und drücken Sie dann die **Eingabetaste**.

   Sie werden aufgefordert, die ursprünglichen Konfigurationseinstellungen des Geräts einzugeben. Detaillierte Informationen zur Vorgehensweise können Sie dem Installationshandbuch entnehmen, das dem Gerät beiliegt. Dieses Handbuch steht auch auf der Juniper-Supportsite (http://www.juniper.net/support/) im PDF-Format zur Verfügung.

Nach dem Abschluss des Initialisierungsvorgangs können Sie auf das neueste IVE-Betriebssystem-Paket aktualisieren und die gespeicherten System- und Benutzerkonfigurationsdateien importieren, um zum letzten funktionstüchtigen Zustand des Geräts zurückzukehren.

HINWEIS: Während des ersten Setups oder der Wiederherstellung der Werkseinstellungen werden möglicherweise IVE-Fehler angezeigt. Bevor das IVE Dienste startet, überwacht es den Netzwerkport für eine Dauer von maximal 120 Sekunden. Das IVE überprüft den Verbindungsstatus und führt einen ARPing-Befehl für das Standardgateway aus. Wenn ein Problem vorliegt, zeigt das IVE nach 5 Sekunden eine mit NIC:..... beginnende Meldung auf der seriellen Konsole an. Wird die Verbindung innerhalb von 120 Sekunden wiederhergestellt, wird der Startprozess fortgesetzt. Wenn die Verbindung nicht wiederhergestellt wird, wird die folgende Meldung angezeigt:

```
Internal NIC: .....[Down code=0x1]
```

Zwei Codes können angezeigt werden:

- 0x1 bedeutet, dass der von der NIC gemeldete Schnittstellenverbindungsstatus weiterhin OFF lautet (z. B. ein abgetrenntes Kabel oder ein am falschen Port angeschlossenes Kabel).
- 0x2 bedeutet, dass das Gateway nicht erreichbar ist. Das IVE startet, es ist aber nicht erreichbar über IP-Adressen, die an diesen Netzwerkport gebunden sind.

Durchführen gängiger Wiederherstellungsvorgänge

Wenn Sie Ihren Administratorbenutzernamen und/oder das Administratorkennwort für das IVE vergessen, sich aufgrund von Konfigurationsfehlern selbst vom Gerät ausgesperrt oder die IP-Adresse der IVE-Appliance geändert haben und nicht mehr auf das Gerät zugreifen können, können Sie die Geräteeinstellungen über die serielle Konsole ändern. Folgen Sie den Anweisungen unter „Herstellen einer Verbindung mit der seriellen Konsole der IVE-Appliance“ auf Seite 389, und wählen Sie dann den gewünschten Konfigurationsvorgang aus.

- **Network Settings and Tools** – Hiermit können Sie die Standardnetzwerkeinstellungen ändern, eine Routingtabelle drucken, den ARP-Cache ausgeben oder leeren, einen anderen Server pingen, die Route zu einem Server verfolgen, statische Routen entfernen und einen ARP-Eintrag hinzufügen.
- **Create admin username and password** – Hiermit können Sie ein neues Super-Administratorkonto erstellen.
- **Display log** – Hiermit können Sie die Systemkonfiguration, Benutzerprotokolle oder Protokolle des Administratorzugriffs über die serielle Konsole anzeigen. Nach dem Anzeigen der Protokolle müssen Sie „q“ eingeben, um wieder die Optionen der seriellen Konsole anzuzeigen.

- **System Operations** – Hiermit können Sie die IVE-Appliance ohne Verwendung der Webkonsole neu starten, herunterfahren oder starten, und Sie können ein Rollback durchführen oder die Werkseinstellungen wiederherstellen.

- **Toggle password protection for the console** – Hiermit können Sie den Kennwortschutz für die serielle Konsole aktivieren und deaktivieren. Wenn Sie diese Option auf „on“ setzen, ist der Zugriff nur Super-Administratoren gestattet.

- **Create a Super Admin session** – Hiermit können Sie auch dann eine Wiederherstellungssitzung auf der Webkonsole erstellen, wenn Sie die IVE-Appliance zum Blockieren des gesamten Administratorzugriffs konfiguriert haben. Wenn Sie diese Option aktivieren, generiert die Appliance einen temporären Token, der drei Minuten gültig ist. Geben Sie den folgenden URL in ein Browserfenster ein: https://<ive-host>/dana-na/auth/recover.cgi. Geben Sie dann bei der entsprechenden Aufforderung den temporären Token ein, um sich an der Webkonsole anzumelden.

HINWEIS: Wenn Sie diese Option auswählen, sperrt die IVE-Appliance alle weiteren Administratoren. Diese können sich dann nicht an der Webkonsole anmelden, bis Sie sich am angegebenen URL angemeldet und die Sitzung mit ihrem Token gestartet haben. Die Appliance sperrt weitere Anmeldeversuche, so dass Sie vom IVE erkannte Konfigurationsprobleme beheben können, ohne dadurch in einer anderen Sitzung Störungen zu verursachen.

- **System Snapshot** – Hiermit können Sie ohne Verwendung der Webkonsole einen Systemsnapshot erstellen. Wenn Sie diese Option auswählen, nimmt das IVE den Snapshot sofort auf. Sie können die Snapshotdatei dann via SCP an ein Remotesystem senden. Das System fordert Sie auf, den Zielserverport, die Benutzer-ID, das Kennwort und den Zielpfad des Remoteverzeichnisses anzugeben.

HINWEIS: Wenn Sie die Snapshotdatei nicht an ein Remotesystem senden möchten, speichert das IVE die Datei lokal. Bei der nächsten Anmeldung an der Webkonsole enthält die Registerkarte **System Snapshot** einen Link zu der Snapshotdatei. Weitere Informationen zum Aufnehmen von Snapshots über die Webkonsole finden Sie unter „Registerkarte „System Snapshot““ auf Seite 382.

Anhang B

Schreiben benutzerdefinierter Ausdrücke

Dieser Abschnitt ist in folgende Themen untergliedert:

- „Benutzerdefinierte Ausdrücke“ auf Seite 397
- „Systemvariablen und Beispiele“ auf Seite 401

Benutzerdefinierte Ausdrücke

Mit dem IVE können Sie benutzerdefinierte Ausdrücke schreiben, die in Rollenzuordnungsregeln, Ressourcenrichtlinien und Protokollfilterabfragen ausgewertet werden. Ein *benutzerdefinierter Ausdruck* ist eine Kombination von Variablen, die das IVE als boolesches Objekt als „true“ (wahr), „false“ (falsch) oder „error“ (Fehler) auswertet. Mithilfe von benutzerdefinierten Ausdrücken können Sie komplexe Bedingungen für Richtlinienauswertung und Protokollabfragen erstellen, die die Ressourcenzugriffskontrolle verbessern und erleichtern.

Sie können benutzerdefinierte Ausdrücke in den folgenden Formaten schreiben:

variable comparisonOperator variable
variable comparisonOperator simpleValue
variable comparisonOperator (simpleValue)
variable comparisonOperator (ORValues)
variable comparisonOperator (ANDValues)
variable comparisonOperator (time **TO** time)
variable comparisonOperator (day **TO** day)
isEmpty (variable)
isUnknown (variable)
(customExpr)
NOT customExpr
! customExpr
customExpr **OR** customExpr
customExpr **||** customExpr
customExpr **AND** customExpr
customExpr **&&** customExpr

Die in diesen benutzerdefinierten Ausdrucksformaten verwendeten Elemente werden in der folgenden Tabelle beschrieben:

Tabelle 22: Elemente von benutzerdefinierten Ausdrücken

variable	Stellt eine Systemvariable dar. Ein Variablenname ist eine durch Punkte getrennte Zeichenfolge. Jede Komponente darf Zeichen aus dem Bereich [a-z A-Z 0-9_] enthalten, darf jedoch nicht mit einer Ziffer [0-9] starten. Bei Variablennamen wird die Groß- und Kleinschreibung nicht berücksichtigt. Systemvariablen, die in Rollenzuordnungsregeln und -ressourcen verwendet werden können, finden Sie unter „Systemvariablen und Beispiele“ auf Seite 401. Zum Schreiben eines benutzerdefinierten Ausdrucks in einem Protokollabfragefeld müssen Sie Systemprotokollvariablen verwenden. Diese Variablen werden im Filtervariablenwörterbuch auf der Seite **Filter** beschrieben (Registerkarte **System > Log/Monitoring > Events** | **User Access** | **Admin Access > Filters**).	
	Maskierte Syntax für Variablen Das IVE unterstützt eine maskierte Syntax für Variablen benutzerdefinierter Ausdrücke, die die Verwendung aller Zeichen außer '.' (Punkt) in Benutzerattributnamen ermöglicht. Um in Attributnamen Escape-Zeichen zu verwenden, maskieren Sie Teile des Variablennamens oder den gesamten Namen mit **{ }** (geschweifte Klammern). Beispielsweise entsprechen sich folgende Ausdrücke: userAttr.{Login-Name} = 'xyz' userAttr.Login{-}Name = 'xyz' {userAttr.Login-Name} = 'xyz' userA{ttr.L}{ogin-}Name = 'xyz'	
	Innerhalb von Maskierungen werden die folgenden Escape-Zeichen unterstützt:	
	\\	steht für \ (umgekehrter Schrägstrich)
	\{	steht für { (linke geschweifte Klammer)
	\}	steht für } (rechte geschweifte Klammer)
	\hh	steht für einen hexadezimalen Wert, wobei hh zwei Zeichen von [0-9A-Fa-f] darstellt
	Beispiele: userAttr.{Tree Frog} = 'kermit' userAttr.{Tree\20Frog} = 'kermit'	
	Hinweise: ■ Die Anzahl der Maskierungen, die in einem Variablennamen verwendet werden können, ist unbegrenzt. ■ Sie können die maskierte Syntax nicht nur mit userAttr.*-Variablen, sondern mit allen Variablen verwenden. ■ Maskierungen aus geschweiften Klammern müssen nur bei benutzerdefinierten Ausdrücken verwendet werden.	
comparisonOperator	kann folgende Werte annehmen:	
	=	gleich – Kann für Zeichenfolgen, Zahlen und DNs verwendet werden

Tabelle 22: Elemente von benutzerdefinierten Ausdrücken (Fortsetzung)

	!=	ungleich – Kann für Zeichenfolgen, Zahlen und DNs verwendet werden
	<	kleiner als – Kann mit Zahlen verwendet werden
	<=	kleiner oder gleich – Kann mit Zahlen verwendet werden
	>	größer als – Kann für Zahlen verwendet werden
	>=	größer oder gleich – Kann für Zahlen verwendet werden
simpleValue	kann folgende Werte annehmen: ■ Zeichenfolge – Zeichenfolge in Anführungszeichen, die Platzhalter enthalten kann ■ IP-Adresse – a.b.c.d ■ Subnetz – a.b.c.d/Subnetz Anzahl Bits oder a.b.c.d/Netmask ■ Zahl – positive oder negative Ganzzahl ■ Tag — SUN MON TUE WED THU FRI SAT Hinweise zu Zeichenfolgen: ■ Eine Zeichenfolge kann alle Zeichen außer <nl> (neue Zeile) und <cr> (Wagenrücklauf) enthalten. ■ Zeichenfolgen können beliebig lang sein. ■ Bei Zeichenfolgenvergleichen wird die Groß- und Kleinschreibung nicht berücksichtigt. ■ Zeichenfolgen können in einfache oder doppelte Anführungszeichen gesetzt werden. Eine Zeichenfolge in Anführungsstrichen kann Platzhalter enthalten, d. h. Sternchen (*), Fragezeichen (?) und eckige Klammern ([ ]). Siehe „Platzhalterabgleich“ auf Seite 400. ■ Vergleiche vom Typ *variable comparisonOperator variable* werden ohne Platzhalterabgleich ausgewertet. ■ Verwenden Sie einen umgekehrten Schrägstrich als Escape-Zeichen für die folgenden Zeichen: einfaches Anführungszeichen (') – \' doppeltes Anführungszeichen (") – \" umgekehrter Schrägstrich (\) – \\ Hexadezimalzahl – \hh [0-9a-fA-F] Hinweis zum Tag: Tag- und Zeitvergleiche werden in der Zeitzone des IVE ausgewertet. Berechnungen der Tagesbereiche (Tag TO Tag) beginnen mit dem ersten angegebenen Tag und werden schrittweise ausgeführt, bis der zweite angegebene Tag erreicht wird. In Berechnungen für Zeitbereiche (Zeit TO Zeit) muss der erste Wert zeitlich vor dem zweiten Wert liegen. Nur Zeitvariablen können mit Tages- und Zeitwerten verglichen werden. Zeitvariablen sind: time.* und loginTime.*	

Tabelle 22: Elemente von benutzerdefinierten Ausdrücken (Fortsetzung)

Zeit	ist die Uhrzeit in einem der folgenden Formate: SS:MM – 24-Stunden-Format SS:MMam – 12-Stunden-Format SS:MMpm – 12-Stunden-Format S:MM – 24-Stunden-Format S:MMam – 12-Stunden-Format S:MMpm – 12-Stunden-Format Tag- und Zeitvergleiche werden in der Zeitzone des IVE ausgewertet. Berechnungen der Tagesbereiche (Tag TO Tag) beginnen mit dem ersten angegebenen Tag und werden schrittweise ausgeführt, bis der zweite angegebene Tag erreicht wird. In Berechnungen für Zeitbereiche (Zeit TO Zeit) muss der erste Wert zeitlich vor dem zweiten Wert liegen. Nur Zeitvariablen können mit Tages- und Zeitwerten verglichen werden. Zeitvariablen sind: time.* und loginTime.*
ORValue	ist eine Zeichenfolge, die OR-Vergleiche enthält: *variable comparisonOperator* (Zahl OR Zahl ...) variable comparisonOperator (Zeichenfolge OR Zeichenfolge...)
ANDValue	ist eine Zeichenfolge, die AND-Vergleiche enthält: *variable comparisonOperator* (Zahl AND Zahl...) *variable comparisonOperator* (Zeichenfolge AND Zeichenfolge...)
isEmpty	ist eine Funktion, die eine einzelne Variable als Argument nimmt und einen booleschen Wert zurückgibt. isEmpty() ist „true“, wenn die Variable unbekannt ist, eine Länge von Null hat oder Zeichenfolgen der Länge Null bzw. leere Listen enthält. Beispiel: isEmpty(userAttr.terminationDate)
isUnknown	ist eine Funktion, die eine einzelne Variable als Argument nimmt und einen booleschen Wert zurückgibt. isUnknown() ist „true“, wenn die Variable nicht definiert ist. Benutzerattribute (userAttr.*-Variablen) sind unbekannt, wenn das Attribut nicht in LDAP definiert ist oder wenn der Attribut-Lookup fehlschlägt (wenn z. B. der LDAP-Server außer Betrieb ist). Beispiel: isUnknown(userAttr.bonusProgram)
NOT, !	ist der Vergleichsoperator für die logische Negation. Der negierte Ausdruck ergibt „true“, wenn der benutzerdefinierte Ausdruck „false“ ist und „false“, wenn der benutzerdefinierte Ausdruck „true“ ist. Die Operatoren NOT, AND und OR werden von der höchsten zur niedrigsten Priorität in folgender Rangfolge ausgewertet: NOT (von rechts), AND (von links), OR (von links).
OR, ||	ist der logische Operator OR oder ||, die äquivalent sind. Die Operatoren NOT, AND und OR werden von der höchsten zur niedrigsten Priorität in folgender Rangfolge ausgewertet: NOT (von rechts), AND (von links), OR (von links).
AND, &&	ist der logische Operator AND oder &&, die äquivalent sind. Die Operatoren NOT, AND und OR werden von der höchsten zur niedrigsten Priorität in folgender Rangfolge ausgewertet: NOT (von rechts), AND (von links), OR (von links).
customExpr	ist ein in der Syntax für benutzerdefinierte Ausdrücke geschriebener Ausdruck (siehe oben).

Platzhalterabgleich

In einer Zeichenfolge, die in Anführungszeichen eingeschlossen ist, können Platzhalter verwendet werden. Folgende Platzhalter werden unterstützt:

- **Sternchen (*)** – Ein Sternchen steht für eine beliebige Folge von null oder mehr Zeichen.
- **Fragezeichen (?)** – Ein Fragezeichen steht für ein einzelnes Zeichen.

- **Eckige Klammern ([ ])** – Eckige Klammern stehen für ein Zeichen aus einem Bereich möglicher Zeichen, der zwischen den Klammern angegeben wird. Zwei durch einen Bindestrich (-) getrennten Zeichen stehen für die beiden Zeichen und die lexikalisch dazwischen liegenden Zeichen. Beispiel: 'dept[0-9]' steht anstelle der Zeichenfolgen „dept0“, „dept1“ usw. bis einschließlich „dept9“.

Die Escape-Zeichen für Platzhalter sind eckige Klammern. So ergibt der Ausdruck ' userAttr.x = "value[*]" ' beispielsweise „true“, wenn das Attribut x genau gleich „value*“ ist.

DN-Variablen

Sie können einen definierten Namen (Distinguished Name, DN) mit einem anderen DN oder einer Zeichenfolge vergleichen, das IVE ignoriert jedoch Platzhalter, Leerzeichen und Groß-/Kleinschreibung. Das IVE berücksichtigt jedoch die Reihenfolge von DN-Schlüsseln.

Wenn das IVE einen Ausdruck für einen DN mit einer Zeichenfolge vergleicht, konvertiert es die Zeichenfolge in einen definierten Namen (DN), bevor es den Ausdruck auswertet. Kann das IVE die Zeichenfolge aufgrund fehlerhafter Syntax nicht konvertieren, schlägt der Vergleich fehl. DN-Variablen sind:

- userDN
- certDN
- certIssuerDN

Systemvariablen und Beispiele

Die folgende Tabelle enthält die Systemvariablen und ihre Definition, Beispiele für jede Systemvariable und Verwendungsbeispiele.

HINWEIS: Diese Liste enthält keine Variablen, die in einer Filterabfrage oder einem Exportformat für ein Systemprotokoll verwendet werden.

Tabelle 23: Systemvariablen und Beispiele

Variable	Beschreibung	Beispiel
authMethod Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Zum Authentifizieren eines Benutzers verwendete Authentifizierungsmethode.	authMethod = ‘ACE Server’
cacheCleanerStatus Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Status von Cache Cleaner. Mögliche Werte: 1 - wenn sie ausgeführt wird 0 - wenn sie nicht ausgeführt wird	cacheCleanerStatus = 1 cacheCleanerStatus = 0

Tabelle 23: Systemvariablen und Beispiele (Fortsetzung)

Variable	Beschreibung	Beispiel
certAttr. < cert-attr > Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ LDAP-Konfiguration ■ Felder für SSO-Parameter	Attribute eines clientseitigen Zertifikats. Beispiele für certAttr-Attribute: C - Country (engl. für Land) CN - Common Name (engl. für allgemeiner Name) description - Beschreibung emailAddress - E-Mail-Adresse GN - Given Name (engl. für Vorname) initials - Initialen L - Locality Name (engl. für Ortsname) O - Organization (engl. für Organisation) OU - Organizational Unit (engl. für Organisationseinheit) SN - Surname (engl. für Nachname) serialNumber- Serial Number (engl. für Seriennummer) ST - State/Province (Bundesland/Kanton) title - Titel UI - Unique Identifier (engl. für eindeutiger Bezeichner) Mithilfe dieser Variable können Sie überprüfen, ob der Client des Benutzers über ein clientseitiges Zertifikat mit den angegebenen Werten verfügt.	certAttr.OU = 'Retail Products Group'
certAttr.altName. < Alt-attr > Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ LDAP-Konfiguration ■ Felder für SSO-Parameter ■	Wert des alternativen Namens des Subjekts aus einem clientseitigen Zertifikat, wobei *< Alt-attr >* folgende Werte annehmen kann: .Email .dirNameText .DNS .URI .ipAddress .registeredId	certAttr.altName.email = „joe@company.com“ certAttr.altName.dirNameText = "cn = joe, ou = company, o = com" certAttr.altName.ipAddress = 10.10.83.2
certAttr.serialNumber Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ LDAP-Konfiguration ■ Felder für SSO-Parameter	Seriennummer eines Clientzertifikats. Beachten Sie, dass alle Zeichen außer [0-9 a-f A-F] aus einer Zeichenfolge vor dem Vergleich mit certAttr.SN entfernt werden. Platzhalter werden nicht unterstützt.	certAttr.SerialNumber = userAttr.certSerial certAttr.SerialNumber = „6f:05:45:ab“

Tabelle 23: Systemvariablen und Beispiele (Fortsetzung)

Variable	Beschreibung	Beispiel
certDN Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	DN des Clientzertifikat-Subjekts. Platzhalter sind nicht zulässig.	certDN = 'cn = John Harding,ou = eng,c = Company' certDN = userDN *(DN des Zertifikat-Subjekts wird mit dem DN des LDAP-Benutzers abgeglichen)* certDN = userAttr.x509SubjectName certDN = ('cn = John Harding,ou = eng,c = Company' or 'cn = Julia Yount,ou = eng,c = Company')
certDN. < subject-attr > Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ LDAP-Konfiguration ■ Felder für SSO-Parameter	Beliebige Variable aus dem DN des Clientzertifikat-Subjekts, wobei *subject-attr* der Name des RDN-Schlüssels ist. Kann zum Testen verschiedener DN-Attribute in einem Standard-x.509-Zertifikat verwendet werden.	certDN.OU = ‚company‘ certDN.E = ‚joe@company.com‘ certDN.ST = ‚CA‘
certDNText Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Benutzer-DN eines Clientzertifikats. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	certDNText = 'cn = John Harding,ou = eng,c = Company'
certIssuerDN Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Subjekt-DN des Clientzertifikat-Ausstellers. Diese Variable verhält sich wie ein Standard-DN-Attribut (wie z. B. CertDN). Platzhalter sind nicht zulässig.	certIssuerDN = 'cn = John Harding,ou = eng,c = Company' certIssuerDN = userAttr.x509Issuer certIssuerDN = ('ou = eng,c = Company' or 'ou = operations,c = Company')
certIssuerDN. < issuer-attr > Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Beliebige Variable aus dem Subjekt-DN des Clientzertifikat-Ausstellers, wobei *issuer-attr* der Name des RDN-Schlüssels ist.	certIssuerDN.OU = ‚company‘ certIssuerDN.ST = ‚CA‘
certIssuerDNText Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Subjekt-DN des Clientzertifikat-Ausstellers. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	certIssuerDNText = 'cn = John Harding,ou = eng,c = Company'

Tabelle 23: Systemvariablen und Beispiele (Fortsetzung)

Variable	Beschreibung	Beispiel
group. < group-name > Verfügbar in: Rollenzuordnungsregeln Ressourcenrichtlinienregeln **Hinweis:** Nur die für Rollenzuordnungsregeln ausgewerteten Gruppen sind in den detaillierten Regeln (Bedingungen) in den Ressourcenrichtlinien verfügbar. Wir empfehlen die Verwendung der Gruppenvariable anstelle von group. < group-name > , das nur aus Gründen der Abwärtskompatibilität unterstützt wird.	Von der Bereichsauthentifizierung oder dem Verzeichnisserver bereitgestellte Gruppenmitgliedschaft von Benutzern.	group.preferredPartner group.goldPartner or group.silverPartner group.employees and time.month = 9 *Beispiele für Kombinationen:* *Erlaubt alle Partner mit dem Status "Aktiv" von Montag bis Freitag, jedoch bevorzugte Partner von Montag bis Samstag:* ((group.partners and time = (Mon to Fri)) or (group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active' **Hinweis:** Leerzeichen werden nicht unterstützt, z. B.: group.sales managers.
groups Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Von der Bereichsauthentifizierung oder dem Verzeichnisserver bereitgestellte Gruppenlisten. **HINWEIS:**Sie können im Gruppennamen alle Zeichen verwenden. Platzhalterzeichen werden nicht unterstützt.	groups = ('sales managers')
hostCheckerPolicy Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Vom Client erfüllte Host Checker-Richtlinien.	hostCheckerPolicy = ('Norton' and 'Sygate') and cacheCleanerStatus = 1
loginHost Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ LDAP-Konfiguration ■ Felder für SSO-Parameter	Der Hostname oder die IP-Adresse des Browsers, mit dem auf das IVE zugegriffen wird.	loginHost = 10.10.10.10
loginTime Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Die Uhrzeit, zu der der Benutzer seine Anmeldeinformationen an das IVE sendet. Die Zeit basiert auf der IVE-Zeit. **HINWEIS:** Bei Verwendung dieser Variablen in einem SSO-Parameterfeld gibt die Variable die „UNIX string time“ zurück (Zeichenfolge mit der Uhrzeit).	loginTime = (8:00am to 5:00pm) loginTime = (Mon to Fri)
loginTime.day Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Tag des Monats, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „day“ einen Wert von 1-31 annehmen kann. Die Zeit basiert auf der IVE-Zeit.	loginTime.day = 3

Tabelle 23: Systemvariablen und Beispiele (Fortsetzung)

Variable	Beschreibung	Beispiel
loginTime.dayOfWeek Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Wochentag, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet. „dayOfWeek“ kann im Bereich [0-6] liegen (0 = Sonntag).	loginTime.dayOfWeek = (0 OR 6) loginTime.dayOfWeek = (1 bis 5) loginTime.dayOfWeek = 5
loginTime.dayOfYear Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der numerische Tag des Jahres, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „dayOfYear“ auf [0-365] gesetzt werden kann.	loginTime.dayOfYear = 100
loginTime.month Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Monat, in dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „month“ auf [1-12] gesetzt werden kann (1 = Januar).	loginTime.month > = 4 AND loginTime.month < = 9
loginTime.year Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Das Jahr, in dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „year“ auf [1900-2999] gesetzt werden kann.	loginTime.year = 2005
loginURL Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ LDAP-Konfiguration ■ Felder für SSO-Parameter	Der URL der Seite, die der Benutzer zur Anmeldung am IVE verwendet hat. Das IVE ruft diesen Wert aus der Spalte „Administrator URLs/User URLs“ auf der Seite „System > Signing In > Sign-in Policies“ der Webkonsole ab.	loginURL = */admin
networkIf Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Die Netzwerkschnittstelle, an der eine Benutzerabfrage empfangen wird. Mögliche Werte: „internal“, „external“	sourceIp = 192.168.1.0/24 und networkIf = internal
ntdomain Verfügbar in: ■ Rollenzuordnungsregeln ■ Felder für SSO-Parameter	Die NetBIOS NT-Domäne, die bei der NT4- und Active Directory-Authentifizierung verwendet wird.	ntdomain = jnpr
ntuser Verfügbar in: ■ Rollenzuordnungsregeln ■ Felder für SSO-Parameter	Der bei der Active Directory-Authentifizierung verwendete NT-Benutzername.	ntuser = jdoe

Tabelle 23: Systemvariablen und Beispiele (Fortsetzung)

Variable	Beschreibung	Beispiel
password **password[1]** **password[2]** Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Das vom Benutzer für den primären Authentifizierungsserver („password“ und „password[1]“) oder den sekundären Authentifizierungsserver („password[2]“) eingegebene Kennwort.	password = A1defo2z
Bereich Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Der Name des Authentifizierungsbereichs, an dem der Benutzer angemeldet ist.	Realm = (‚GoldPartners‘ or ‚SilverPartners‘) *Hinweis: Die Bedingung AND führt zu keinem Ergebnis, da sich ein Benutzer in einer Sitzung nur an einem einzigen Bereich anmelden kann.*
Rolle Verfügbar in: ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Liste aller Benutzerrollen für eine Sitzung. Wenn Sie in SSO alle Rollen an Back-End-Anwendungen senden möchten, verwenden Sie <role *sep* = ";"> – wobei *sep* die Zeichenfolge zum Trennen mehrerer Werte ist. Das IVE unterstützt alle Trennzeichen mit Ausnahme von “ und >.	Role = (‚sales‘ or ‚engineering‘) Role = (‚Sales‘ AND ‚Support‘)
sourceIP Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Die IP-Adresse des Geräts, auf dem sich der Benutzer authentifiziert. Sie können die Netzmaske mit der Bitzahl oder im Netzmaskenformat angeben: '255.255.0.0'	sourceIP = 192.168.10.20 sourceIP = 192.168.1.0/24 und networkIf internal userAttr.dept = ('eng' or 'it') and sourceIP = 10.11.0.0/16 sourceIP = 192.168.10.0/24 *(Klasse C)* *ist identisch mit* sourceIP = 192.168.10.0/255.255.255.0
Zeit Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Die Uhrzeit, zu der die Rollenzuordnungsregel oder die Ressourcenrichtlinienregel ausgewertet wird. Die Uhrzeit kann im 12- oder 24-Stunden-Format angegeben werden.	time = (09:00:00 to 17:00:00) time = (09:00 to 17:00) time = (Mon to Fri) *Beispiele für Kombinationen:* *Erlaubt leitenden Angestellten und deren Assistenten den Zugriff von Montag bis Freitag:* userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri)

Tabelle 23: Systemvariablen und Beispiele (Fortsetzung)

Variable	Beschreibung	Beispiel
time.day Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Tag des Monats, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „day“ einen Wert von 1-31 annehmen kann. Die Zeit basiert auf der IVE-Zeit.	loginTime.day = 3
time.dayOfWeek Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Wochentag, an dem die Rollenzuordnungsregel oder Ressourcenrichtlinie ausgewertet wird. „dayOfWeek“ kann im Bereich [0-6] liegen (0 = Sonntag).	loginTime.dayOfWeek = (0 OR 6) loginTime.dayOfWeek = (1 bis 5) loginTime.dayOfWeek = 5
time.dayOfYear Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Tag im Jahr, an dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. Mögliche Werte sind: 1-365.	time.dayOfYear = 100
time.month Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Monat, in dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. Mögliche Werte sind: 1-12	time.month > = 9 and time.month < = 12 and time.year = 2004 group.employees and time.month = 9
time.year Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Das Jahr, in dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. „year“ kann auf [1900-2999] gesetzt werden	time.year = 2005
user **user[1]** **user[2]** Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	IVE-Benutzername für den primären Authentifizierungsserver („user“ und „user[1]“) oder den sekundären Authentifizierungsserver („user[2]“) des Benutzers. Wird zur Authentifizierung für Active Directory-Server, Domäne und Benutzername verwendet. **HINWEIS:** Wenn Sie eine Domäne in einen Benutzernamen einschließen, müssen zwei Schrägstriche zwischen Domäne und Benutzer eingefügt werden. Beispiel: user = 'ihrefirma.net\\joeuser'.	user = 'steve' user = 'domain\\steve'
username **username[1]** **username[2]** Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	IVE-Benutzername für den primären Authentifizierungsserver („username“ und „username[1]“) oder den sekundären Authentifizierungsserver („username[2]“) des Benutzers. Wenn sich der Benutzer an einem Zertifikat-Authentifizierungsserver anmeldet, ist sein IVE-Benutzername derselbe wie CertDN.cn.	username = 'steve' and time = mon username = 'steve' username = 'steve*' username = ('steve' oder '*jankowski')
userAgent Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Die Benutzer-Agent-Zeichenfolge des Browsers.	Die Benutzer-Agent-Zeichenfolge des Browsers.

Tabelle 23: Systemvariablen und Beispiele (Fortsetzung)

Variable	Beschreibung	Beispiel
userAttr. < auth-attr > Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Von einem LDAP- oder RADIUS-Authentifizierungsserver oder -Verzeichnisserver abgerufene Benutzerattribute.	userAttr.building = ('HQ*' or 'MtView[1-3]') userAttr.dept = ('sales' and 'eng') userAttr.dept = ('eng' or 'it' or 'custsupport') userAttr.division = 'sales' userAttr.employeeType != 'contractor' userAttr.salaryGrade > 10 userAttr.salesConfirmed >= userAttr.salesQuota **Negative Beispiele:** userAttr.company != "Acme Inc" or not group.contractors not (user = 'guest' or group.demo) **Beispiele für Kombinationen:** *Erlaubt leitenden Angestellten und deren Assistenten den Zugriff von Montag bis Freitag:* userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri) *Erlaubt alle Partner mit dem Status "Aktiv" von Montag bis Freitag, jedoch bevorzugte Partner von Montag bis Samstag:* ((group.partners and time = (Mon to Fri)) or (group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active'
userDN Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln	Der Benutzer-DN von einem LDAP-Server. Wenn der Benutzer durch den LDAP-Server authentifiziert wird, stammt dieser DN vom Authentifizierungsserver, andernfalls stammt der DN vom Verzeichnis-/Attributserver des Bereichs. Platzhalter sind nicht zulässig.	userDN = 'cn=John Harding,ou=eng,c=Company' userDN = certDN

Tabelle 23: Systemvariablen und Beispiele (Fortsetzung)

Variable	Beschreibung	Beispiel
userDN. < user-attr > Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Beliebige Variable aus dem Benutzer-DN, wobei *user-attr* der Name des RDN-Schlüssels ist.	Beliebige Variable aus dem Benutzer-DN, wobei *user-attr* der Name des RDN-Schlüssels ist.
userDNText Verfügbar in: ■ Rollenzuordnungsregeln ■ Ressourcenrichtlinienregeln ■ Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Benutzer-DN. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	userDNText = 'cn = John Harding,ou = eng,c = Company'

Anhang C

Installation von clientseitigen Anwendungen

In diesem Abschnitt werden die zum Installieren und Ausführen verschiedener clientseitiger Komponenten von IVE erforderlichen Berechtigungen beschrieben. Aufgelistet werden auch die Paketdateinamen, die das IVE zum Installieren der clientseitigen Komponenten verwendet, die von den Paketen installierten und deinstallierten Dateien sowie die auf dem Benutzersystem vorgenommenen Registrierungsänderungen. Dieser Abschnitt umfasst folgende Themen:

- „Erforderliche Berechtigungen zum Installieren und Ausführen von Anwendungen“ auf Seite 411
- „Anwendungsdateiverzeichnisse“ auf Seite 412

Erforderliche Berechtigungen zum Installieren und Ausführen von Anwendungen

In den folgenden Tabellen werden die Berechtigungen erläutert, die zum Installieren und Ausführen der folgenden clientseitigen IVE-Komponenten mithilfe von ActiveX, des ActiveX-Installationsdienstes und der Java-Mechanismen von IVE erforderlich sind:

- „Network Connect“ auf Seite 412
- „Host Checker“ auf Seite 412
- „Cache Cleaner“ auf Seite 412

Sofern zutreffend, enthalten die Tabellen auch Links zu Themen, in denen Sie ausführliche Informationen zu den von IVE zur Installation und Ausführung der clientseitigen Anwendungen verwendeten Komponenten finden.

Tabelle 24: Network Connect

Aktion	ActiveX Windows	ActiveX Installer Service Windows	Java Windows	Java Mac/Linux	Weitere Informationen
Installieren	Admin	Eingeschränkt, Hauptbenutzer oder Admin	Admin	Nicht zutreffend	Siehe „Network Connect“ auf Seite 415.
Ausführen	Hauptbenutzer oder Admin	Eingeschränkt, Hauptbenutzer oder Admin	Hauptbenutzer oder Admin	Nicht zutreffend	Siehe „Network Connect“ auf Seite 415.

Tabelle 25: Host Checker

Aktion	ActiveX Windows	ActiveX Installer Service Windows	Java Windows	Java Mac/Linux	Weitere Informationen
Installieren	Admin	Eingeschränkt, Hauptbenutzer oder Admin	Eingeschränkt, Hauptbenutzer oder Admin	Nicht zutreffend	Siehe „Host Checker“ auf Seite 414.
Ausführen	Eingeschränkt, Hauptbenutzer oder Admin	Eingeschränkt, Hauptbenutzer oder Admin	Eingeschränkt, Hauptbenutzer oder Admin	Nicht zutreffend	Siehe „Host Checker“ auf Seite 414.

Tabelle 26: Cache Cleaner

Aktion	ActiveX Windows	ActiveX Installer Service Windows	Java Windows	Java Mac/Linux	Weitere Informationen
Installieren	Admin	Eingeschränkt, Hauptbenutzer oder Admin	Eingeschränkt, Hauptbenutzer oder Admin	Nicht zutreffend	Siehe „Cache Cleaner“ auf Seite 415.
Ausführen	Eingeschränkt, Hauptbenutzer oder Admin	Eingeschränkt, Hauptbenutzer oder Admin	Eingeschränkt, Hauptbenutzer oder Admin	Nicht zutreffend	Siehe „Cache Cleaner“ auf Seite 415.

Anwendungsdateiverzeichnisse

In diesem Abschnitt werden die Komponenten beschrieben, mit denen das IVE die clientseitigen Anwendungen installiert und ausführt. Im Folgenden werden die Komponentennamen, die Speicherorte der Installationsprogramme, die Protokollverzeichnisse sowie die Registrierungsänderungen beschrieben, die von den Komponenten während der Installation vorgenommen werden:

- „NeoterisSetup Control“ auf Seite 413
- „Host Checker“ auf Seite 414

- „Cache Cleaner“ auf Seite 415
- „Network Connect“ auf Seite 415

NeoterisSetup Control

Wenn Sie eine Windows-basierte IVE-Clientanwendung auf dem Windows-System eines Benutzers installieren, verwendet das IVE eine ActiveX-Komponente namens NeoterisSetup Control, um das Installationsprogramm der Clientanwendung auf das System des Benutzers herunterzuladen und den Installationsvorgang zu verwalten.

Tabelle 27: NeoterisSetup Control

Anforderungen für das Paket	Anwendbarer Wert
Speicherort der Paketdatei:	C:\WINDOWS\Übertragene Programmdateien\NeoterisSetupDLL.cab Windows 2000: C:\WINNT\Übertragene Programmdateien\NeoterisSetupDLL.cab
Registrierungsänderungen:	Keine
Zusätzlich installierte Dateien:	NeoterisSetup.inf NeoterisSetup.log NeoterisSetup.ocx NeoterisSetupDll.dll setupResource_de.dll setupResource_en.dll setupResource_fr.dll setupResource_ja.dll setupResource_zh.dll setupResource_zn_cn.dll
Speicherort der zusätzlichen Dateien:	C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Juniper Networks\Setup C:\WINDOWS\Übertragene Programmdateien
Nach Deinstallation verbleibende Dateien:	Wenn das ActiveX-Steuerelement aus IE gelöscht wird, verbleiben folgende Dateien auf dem System: NeoterisSetup.log NeoterisSetup.ocx setupResource_es.dll setupResource_ko.dll
Speicherort der Protokolldatei:	C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Juniper Networks\Setup

Host Checker

Zum Ausführen von Host Checker lädt das IVE das Paket **neoHCSetup.exe.cab** auf den Client des Benutzers herunter. Dieses Paket übernimmt das Herunterladen weiterer Dateien auf das System, die für Host Checker erforderlich sind.

Tabelle 28: Host Checker

Anforderungen für das Paket	Anwendbarer Wert
Speicherort der Paketdatei:	C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp\neoHCSetup.exe.cab
Registrierungsänderungen:	Zeichenfolgen: LogFile und level werden festgelegt in HKEY_CURRENT_USER\SOFTWARE\Juniper\Host Checker\Debug\dsHostChecker Zeichenfolgen: Language und InstallPath werden festgelegt in HKEY_CURRENT_USER\SOFTWARE\Juniper\Host Checker
Zusätzlich installierte Dateien:	dsHostChecker.exe dsHostChecker.log dsHostCheckerResource_de.dll dsHostCheckerResource_en.dll dsHostCheckerResource_es.dll dsHostCheckerResource_fr.dll dsHostCheckerResource_ja.dll dsHostCheckerResource_ko.dll dsHostCheckerResource_zh.dll dsHostCheckerResource_zh_cn.dll psapi.dll neodbg.dll uninstall.exe versionInfo.ini
Speicherort der zusätzlichen Dateien:	C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Juniper Networks\HostChecker
Nach Deinstallation verbleibende Dateien:	Keine
Speicherort der Protokolldatei:	C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Juniper Networks\Host Checker\dsHostChecker.log C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Juniper Networks\hcsetup.log C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Juniper Networks\EPCheck\EPCheck.log

Cache Cleaner

Zum Ausführen von Cache Cleaner lädt das IVE das Paket **neoCacheCleanerSetup.exe.cab** auf den Client des Benutzers herunter. Dieses Paket übernimmt das Herunterladen weiterer Dateien auf das System, die für Cache Cleaner erforderlich sind.

Tabelle 29: Cache Cleaner

Anforderungen für das Paket	Anwendbarer Wert
Speicherort der Paketdatei:	C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp\neoCacheCleanerSetup.exe.cab
Registrierungsänderungen:	Zeichenfolgen: LogFile und level werden festgelegt in HKEY_CURRENT_USER\SOFTWARE\Juniper\Host Checker\Debug\dsCacheCleaner siehe auch „Registerkarte „Cache Cleaner““ auf Seite 220.
Zusätzlich installierte Dateien:	dsCacheCleaner.exe neodbg.dll uninstall.exe versionInfo.ini
Speicherort der zusätzlichen Dateien:	C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Juniper Networks\CacheCleaner <Versionsnummer>
Nach Deinstallation verbleibende Dateien:	Keine
Speicherort der Protokolldatei:	C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Juniper Networks\CacheCleaner <Versionsnummer>\dsCacheCleaner.log

Network Connect

Zum Ausführen von Network Connect lädt das IVE das Paket **NcSetup.exe.cab** auf den Client des Benutzers herunter. Dieses Paket übernimmt das Herunterladen weiterer Dateien auf das System, die für Network Connect erforderlich sind.

Tabelle 30: Network Connect

Anforderungen für das Paket	Anwendbarer Wert
Speicherort der Paketdatei:	C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp\neoNCsetup.exe.cab
Registrierungsänderungen:	**Hinweis:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce muss auf dem Client unverändert bleiben. Andernfalls schlagen die Installation und der Start von Network Connect fehl.
Dateiinstallationsspeicherorte:	C:\Programme\Neoteris\Network Connect C:\<WINDIR>\system32 C:\<WINDIR>\system32\drivers

Tabelle 30: Network Connect (Fortsetzung)

Anforderungen für das Paket	Anwendbarer Wert
Nach dem Herunterladen zusätzlich installierte Dateien:	ncp.dll ncResource_de.dll ncResource_en.dll ncResource_es.dll ncResource_fr.dll ncResource_ja.dll ncResource_ko.dll ncResource_zh.dll ncResource_zh_cn.dll ncsetup.exe ncsvc.exe (C:\<WINDIR>\system32) ncsvc.log ncui.exe neoconn.txt neodbg.dll neosetup.txt nsvcp.sys (C:\<WINDIR>\system32\drivers) uninstall.exe versionInfo.ini
Nach Deinstallation verbleibende Dateien:	ncsvc.log neosetup.txt
Speicherort der Protokolldatei:	C:\Programme\Neoteris\Network Connect

Anhang D

Konfigurieren der Zugriffsverwaltungsbeschränkungen

Ein IVE ermöglicht Ihnen die Sicherung Ihrer Unternehmensressourcen auf drei Ebenen:

- **Bereich** – Auf der Bereichsebene konfigurieren Sie die Anforderungen für die Zugriffsverwaltung in der Authentifizierungsrichtlinie.
- **Rolle** – Auf der Rollenebene konfigurieren Sie die Anforderungen für die Zugriffsverwaltung entweder in den Rollenzuordnungsregeln der Authentifizierungsrichtlinie oder über die Einschränkungsoptionen für die Rolle.
- **Ressourcenrichtlinie** – Auf der Ebene der Ressourcenrichtlinie konfigurieren Sie die Anforderungen für die Zugriffsverwaltung, indem Sie Bedingungen für Rollen schreiben.

Konfigurationsanweisungen für Optionen der Zugriffsverwaltung finden Sie unter:

- „Angeben von IP-Quelladresseinschränkungen“ auf Seite 418
- „Angeben von Browsereinschränkungen“ auf Seite 419
- „Angeben clientseitiger Zertifikateinschränkungen“ auf Seite 421
- „Angeben einer Kennwortlängeneinschränkung“ auf Seite 422
- „Angeben von Host Checker-Einschränkungen“ auf Seite 423
- „Angeben von Cache Cleaner-Einschränkungen“ auf Seite 425

Eine Übersicht finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 38.

IP-Quelladresseinschränkungen

Mit einer Quell-IP-Einschränkung kann gesteuert werden, von welcher IP-Adresse aus Benutzer auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden können.

Angeben von IP-Quelladresseinschränkungen

So geben Sie IP-Quelladresseinschränkungen an:

1. Wählen Sie die Ebene aus, auf der die IP-Einschränkungen implementiert werden sollen:
   - **Rollenebene** – Wählen Sie:
     - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP
     - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Source IP
     - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
     - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Source IP
   - **Ressourcenrichtlinienebene** – Wählen Sie: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*
2. Wählen Sie eine der folgenden Optionen aus:
   - **Users can sign in from any IP address** – Hiermit können sich Benutzer von einer beliebigen IP-Adresse aus beim IVE anmelden, um die Anforderungen für die Zugriffsverwaltung zu erfüllen.
   - **Users can only sign in from the following IP addresses** – Schränkt die Anzahl der IP-Adressen ein, von denen aus sich Benutzer anmelden können, um die Anforderungen für die Zugriffsverwaltung zu erfüllen. Wenn Sie diese Option auswählen, müssen Sie mindestens eine IP-Adresse angeben, da sonst keine IP-Quelladresseinschränkung angewendet werden kann.
   - **Enable administrators to sign in on the external port** – Ermöglicht es Administratoren, sich über die externe Schnittstelle am IVE anzumelden. Der externe Port muss vor der Auswahl dieser Option aktiviert werden.
3. Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Browsereinschränkungen

Mit einer Browsereinschränkung kann gesteuert werden, von welchen Webbrowsern aus Benutzer auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden können. Wenn ein Benutzer versucht, sich im IVE über einen nicht unterstützten Browser anzumelden, schlägt der Anmeldeversuch fehl, und es wird in einer Meldung angezeigt, dass ein nicht unterstützter Browser verwendet wird. Mit dieser Funktion können Sie auch sicherstellen, dass sich Benutzer im IVE über Browser anmelden, die mit Firmenanwendungen kompatibel oder von Firmensicherheitsrichtlinien zugelassen sind.

HINWEIS: Das Feature zur Browsereinschränkung dient nicht als strikte Zugriffssteuerung, da die Zeichenfolgen für Benutzer-Agenten des Browsers von einem technischen Benutzer geändert werden können. Es dient als beratende Zugriffssteuerung für normale Nutzungsszenarien.

Angeben von Browsereinschränkungen

So geben Sie Browsereinschränkungen an:

1. Wählen Sie die Ebene aus, auf der die Browsereinschränkungen implementiert werden sollen:
   - **Bereichsebene** – Wählen Sie:
     - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser
     - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser
   - **Rollenebene** – Wählen Sie:
     - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Browser
     - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
     - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Browser
   - **Ressourcenrichtlinienebene** – Wählen Sie: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*
2. Wählen Sie eine der folgenden Optionen aus:
   - **Allow all users matching any user-agent string sent by the browser** – Ermöglicht Benutzern den Zugriff auf das IVE oder auf Ressourcen mit einem beliebigen unterstützten Webbrowser.

- **Only allow users matching the following User-agent policy** – Ermöglicht Ihnen die Definition von Regeln für die Browserzugriffssteuerung. So erstellen Sie eine Regel:

  i. Geben Sie für **User-agent string pattern** eine Zeichenfolge in folgendem Format ein:

  <browser_zeichenfolge>

  wobei Start (*) ein optionales Zeichen ist, das für ein beliebiges Zeichen steht, und <browser_zeichenfolge> ein Muster darstellt (Groß-/Kleinschreibung wird berücksichtigt), das mit einer Teilzeichenfolge in dem vom Browser gesendeten „user-agent“-Header übereinstimmen muss. Hinweis: Escape-Zeichen (\) können in Browsereinschränkungen nicht hinzugefügt werden.

  ii. Wählen Sie eine der folgenden Optionen aus:

  - **Allow**, um Benutzern die Verwendung eines Browsers mit einem „user-agent“-Header zu ermöglichen, der die Teilzeichenfolge <browser_zeichenfolge> enthält.
  - **Deny**, um Benutzern die Verwendung eines Browsers mit einem „User-Agent“-Header zu verweigern, der die Teilzeichenfolge <browser_zeichenfolge> enthält.

3. Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

HINWEIS:

- Regeln werden der Reihenfolge nach angewendet, d. h., die erste übereinstimmende Regel wird angewendet.
- Bei Literalzeichen in Regeln wird die Groß- und Kleinschreibung beachtet, Leerzeichen sind dabei zulässig.

Die Zeichenfolge *Netscape* findet z. B. alle Zeichenfolgen für Benutzeragenten mit der Teilzeichenfolge Netscape.

Der folgende Regelsatz ermöglicht Ressourcenzugriff nur dann, wenn Benutzer über Internet Explorer 5.5x oder Internet Explorer 6.x angemeldet sind. In diesem Beispiel werden einige wichtige andere Browser als Internet Explorer berücksichtigt, die die Teilzeichenfolge „MSIE“ im „user-agent“-Header senden:

```
*Opera*Deny
*AOL*Deny
*MSIE 5.5*Allow
*MSIE 6.*Allow
* Deny
```

Zertifikateinschränkungen

Legen Sie anhand einer Zertifikateinschränkung fest, dass Clientcomputer über ein gültiges clientseitiges Zertifikat verfügen müssen, um auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden zu können. Wenn Sie dieses Feature verwenden, stellen Sie sicher, dass Sie ein Zertifikat einer Zertifizierungsstelle importieren, um das clientseitige Zertifikat zu überprüfen (wie unter „Registerkarte „Trusted Client CAs““ auf Seite 170 erläutert). Um die Sicherheit dieses Features zu optimieren, sollten die Clienteinstellungen eines Benutzers so festgelegt werden, dass der Benutzer bei jeder Anmeldung ein Kennwort eingeben muss. In der Standardeinstellung wird bei einigen Browserversionen das Zertifikatkennwort gespeichert, d. h. der Benutzer wird nach Installation des Zertifikats nicht zur Eingabe dieser zusätzlichen Anmeldeinformationen aufgefordert.

Angeben clientseitiger Zertifikateinschränkungen

So geben Sie Zertifikateinschränkungen an:

1. Navigieren Sie zu: **System > Configuration > Certificates > Trusted Client CAs**. Geben Sie die gewünschte Stammzertifizierungsstelle für die Überprüfung der auf der Bereichs-, Rollen- und Ressourcenrichtlinienebene aktivierten Clientzertifikateinschränkungen an. Weitere Informationen finden Sie unter „Registerkarte „Trusted Client CAs““ auf Seite 170.

2. Wählen Sie die Ebene aus, auf der die Zertifikateinschränkungen implementiert werden sollen:

   - **Bereichsebene** – Wählen Sie:

     - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate

     - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate

   - **Rollenebene** – Wählen Sie:

     - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Certificate

     - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*

     - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Certificate

   - **Ressourcenrichtlinienebene** – Wählen Sie: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

3. Wählen Sie eine der folgenden Optionen aus:

   - **Allow all users (no client-side certificate required)** – Clients von Benutzern müssen nicht über ein clientseitiges Zertifikat verfügen.

   - **Only allow users with a client-side certificate signed by Certification Authority to sign in** – Legt fest, dass der Client eines Benutzers über ein clientseitiges Zertifikat verfügen muss, um die Anforderungen für die Zugriffsverwaltung zu erfüllen. Um den Zugriff noch weiter einzuschränken, können Sie eindeutige Attribut-Wert-Paare für das Zertifikat festlegen. Beachten Sie, dass das Zertifikat des Benutzers alle von Ihnen definierten Attribute enthält.

4. Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

HINWEIS:

- Alle X.509-DN-Attribute (Distinguished Name) werden unterstützt (z. B. C, CN, L, O, OU).

- Bei den Attribut- und Wertefeldern wird die Groß- und Kleinschreibung nicht beachtet.

- Definieren Sie für jedes Attribut nur einen Wert. Wenn Sie mehrere Werte angeben, kann das clientseitige Zertifikat möglicherweise nicht ordnungsgemäß anhand des Zertifikats der Zertifizierungsstelle authentifiziert werden.

Kennworteinschränkung

Verwenden Sie eine Kennworteinschränkung, um eine Mindestlänge des Kennworts für den Bereich festzulegen.

Angeben einer Kennwortlängeneinschränkung

So geben Sie Kennworteinschränkungen an:

1. Wählen Sie einen Administrator- oder Benutzerbereich aus, für den Sie die Kennworteinschränkungen implementieren wollen.

   Navigieren Sie zu:

   - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password

   - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password

2. Wählen Sie eine der folgenden Optionen aus:

   - **Allow all users (passwords of any length)** – Für Benutzer, die sich beim IVE anmelden, wird keine Kennwortlängeneinschränkung angewendet.

- **Only allow users that have passwords of a minimum length** – Bei dieser Option muss das einzugebende Kennwort eine festgelegte Anzahl von Zeichen lang sein.

3. Aktivieren Sie das Kontrollkästchen **Enable Password Management**, wenn Sie die Kennwortverwaltung aktivieren möchten. Zusätzlich müssen Sie die Kennwortverwaltung auf der Konfigurationsseite des IVE-Authentifizierungsservers (lokaler Authentifizierungsserver) konfigurieren.

4. Wenn Sie einen sekundären Authentifizierungsserver aktiviert haben, legen Sie Beschränkungen für die Kennwortlänge mithilfe von Schritt 2 als Anhaltspunkt fest.

5. Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

HINWEIS: Für das IVE müssen die auf der Anmeldeseite eingegebenen Benutzerkennwörter standardmäßig mindestens vier Zeichen lang sein. Für den zur Überprüfung der Anmeldeinformationen eines Benutzers verwendeten Authentifizierungsserver ist unter Umständen eine andere Mindestlänge erforderlich. Für die lokale Authentifizierungsdatenbank von IVE müssen die Benutzerkennwörter beispielsweise mindestens sechs Zeichen lang sein.

Host Checker-Einschränkungen

Legen Sie wie unter „Host Checker – Übersicht“ auf Seite 75 beschrieben anhand einer Host Checker-Einschränkung fest, dass Clientcomputer die angegebenen Host Checker-Richtlinien erfüllen müssen, um auf eine IVE-Anmeldeseite oder eine Ressourcenrichtlinie zugreifen oder einer Rolle zugeordnet werden zu können.

Angeben von Host Checker-Einschränkungen

So geben Sie Host Checker-Einschränkungen an:

1. Navigieren Sie zu: **Signing In** > **End Point** > **Host Checker**. Legen Sie globale Optionen für Host Checker fest, die auf alle Benutzer angewendet werden, die gemäß einer Authentifizierungsrichtlinie oder einer Rollenzuordnungsregel Host Checker erfordern. Weitere Informationen finden Sie unter „Registerkarte „Host Checker““ auf Seite 206.

2. Gehen Sie folgendermaßen vor, wenn Sie Host Checker auf der *Bereichsebene* implementieren möchten:

   a. Navigieren Sie zu:

      - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Host Checker

      - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Host Checker

b. Wählen Sie eine der folgenden Optionen für alle verfügbaren Richtlinien oder für einzelne Richtlinien in der Spalte **Available Policies** aus:

- **Evaluate Policies** – Wertet die Richtlinie aus, ohne sie auf dem Client zu erzwingen und lässt Benutzerzugriff zu. Bei dieser Option erfüllt der Benutzer die Zugriffsvoraussetzungen auch dann, wenn Host Checker nicht installiert ist.

- **Require and Enforce** – Erfordert und erzwingt die Richtlinie auf dem Client, damit der Benutzer sich im angegebenen Bereich anmelden kann. Hier müssen von Host Checker die festgelegten Host Checker-Richtlinien ausgeführt werden, damit der Benutzer die Zugriffsvoraussetzungen erfüllt. Das IVE muss Host Checker auf den Clientcomputer herunterladen. Wenn Sie diese Option für die Authentifizierungsrichtlinie eines Bereichs auswählen, lädt das IVE Host Checker auf den Clientcomputer herunter, nachdem der Benutzer authentifiziert, aber bevor er Rollen im System zugeordnet wurde. Durch Auswahl dieser Option wird automatisch die Option **Evaluate Policies** aktiviert.

3. Gehen Sie folgendermaßen vor, wenn Sie Host Checker auf der *Rollenebene* implementieren möchten:

   a. Navigieren Sie zu:

   - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Host Checker

   - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Host Checker

   b. Wählen Sie eine der folgenden Optionen aus:

   - **Allow all users** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn Host Checker nicht installiert ist.

   - **Allow only users whose workstations meet the requirements specified by the following** [Richtlinien] – Der Benutzer erfüllt die Zugriffsvoraussetzungen nur, wenn Host Checker die angegebenen Host Checker-Richtlinien ausführt.

Cache Cleaner-Einschränkungen

Legen Sie wie unter „Cache Cleaner – Übersicht“ auf Seite 87 beschrieben anhand einer Cache Cleaner-Einschränkung fest, dass Clientcomputer die angegebenen Cache Cleaner-Richtlinien erfüllen müssen, um auf eine IVE-Anmeldeseite oder eine Ressourcenrichtlinie zugreifen oder einer Rolle zugeordnet werden zu können.

Angeben von Cache Cleaner-Einschränkungen

So geben Sie Cache Cleaner-Einschränkungen an:

1. Navigieren Sie zu: **Signing In > End Point > Cache Cleaner**. Legen Sie globale Optionen für Cache Cleaner fest, die auf alle Benutzer angewendet werden, die gemäß einer Authentifizierungsrichtlinie, einer Rollenzuordnungsregel oder einer Ressourcenrichtlinie Cache Cleaner erfordern. Weitere Informationen finden Sie unter „Registerkarte „Cache Cleaner““ auf Seite 220.

2. Gehen Sie folgendermaßen vor, wenn Sie Cache Cleaner auf der *Bereichsebene* implementieren möchten:

   a. Navigieren Sie zu: Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Cache Cleaner

   b. Wählen Sie eine der folgenden Optionen aus:

      - **Disable Cache Cleaner** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn Cache Cleaner nicht installiert ist oder ausgeführt wird.

      - **Just load Cache Cleaner** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn Cache Cleaner nicht ausgeführt wird. Die Anwendung muss jedoch für eine spätere Verwendung verfügbar sein. Wenn Sie diese Option für die Authentifizierungsrichtlinie eines Bereichs auswählen, wird Cache Cleaner von IVE auf den Clientcomputer heruntergeladen, nachdem der Benutzer authentifiziert, aber bevor er Rollen im System zugeordnet wurde.

      - **Load and enforce Cache** – Der Benutzer erfüllt die Zugriffsanforderungen nur, wenn Cache Cleaner von IVE heruntergeladen und ausgeführt wird. Wenn Sie diese Option für die Authentifizierungsrichtlinie eines Bereichs auswählen, wird Cache Cleaner von IVE auf den Clientcomputer heruntergeladen, bevor der Benutzer auf die IVE-Anmeldeseite zugreifen kann.

3. Gehen Sie folgendermaßen vor, wenn Sie Cache Cleaner auf der *Rollenebene* implementieren möchten:

   a. Navigieren Sie zu:

      - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Cache Cleaner

      - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Cache Cleaner

   b. Aktivieren Sie **Enable Cache Cleaner**. Cache Cleaner muss ausgeführt werden, damit der Benutzer die Zugriffsanforderungen erfüllt.

Anhang E

Benutzerfehlermeldungen

Dieser Abschnitt enthält die Dokumentation für Endbenutzerfehlermeldungen.

Fehlermeldungen in Network Connect

Dieser Abschnitt behandelt Network Connect-Fehlermeldungen für die folgenden Umgebungen:

- „Windows-Fehlermeldungen“ auf Seite 427
- „Macintosh-Fehlermeldungen“ auf Seite 442

Windows-Fehlermeldungen

Dieser Abschnitt behandelt Network Connect-Fehlermeldungen für Windows:

- „nc.windows.app.1001“ auf Seite 429
- „nc.windows.app.1002“ auf Seite 429
- „nc.windows.app.1003“ auf Seite 429
- „nc.windows.app.1004“ auf Seite 430
- „nc.windows.app.1005“ auf Seite 430
- „nc.windows.app.1006“ auf Seite 430
- „nc.windows.app.1007“ auf Seite 430
- „nc.windows.app.1008“ auf Seite 431
- „nc.windows.app.1009“ auf Seite 431
- „nc.windows.app.1010“ auf Seite 431
- „nc.windows.app.1011“ auf Seite 431
- „nc.windows.app.1012“ auf Seite 432
- „nc.windows.app.1013“ auf Seite 432

- „nc.windows.app.1014“ auf Seite 432
- „nc.windows.app.1015“ auf Seite 432
- „nc.windows.app.1016“ auf Seite 433
- „nc.windows.app.1017“ auf Seite 433
- „nc.windows.app.1018“ auf Seite 433
- „nc.windows.app.1019“ auf Seite 434
- „nc.windows.app.1020“ auf Seite 434
- „nc.windows.app.1021“ auf Seite 434
- „nc.windows.app.1022“ auf Seite 434
- „nc.windows.app.1023“ auf Seite 435
- „nc.windows.app.1024“ auf Seite 435
- „nc.windows.app.1025“ auf Seite 435
- „nc.windows.app.1026“ auf Seite 435
- „nc.windows.app.1027“ auf Seite 435
- „nc.windows.app.1028“ auf Seite 436
- „nc.windows.app.1029“ auf Seite 436
- „nc.windows.app.1030“ auf Seite 436
- „nc.windows.app.1031“ auf Seite 436
- „nc.windows.app.1032“ auf Seite 437
- „nc.windows.app.1033“ auf Seite 437
- „nc.windows.app.1034“ auf Seite 437
- „nc.windows.app.1035“ auf Seite 437
- „nc.windows.app.1036“ auf Seite 438
- „nc.windows.app.1037“ auf Seite 438
- „nc.windows.app.1038“ auf Seite 438
- „nc.windows.app.1039“ auf Seite 438
- „nc.windows.app.1040“ auf Seite 438
- „nc.windows.gina.1001“ auf Seite 439

- „nc.windows.gina.1002“ auf Seite 439
- „nc.windows.gina.1003“ auf Seite 439
- „nc.windows.gina.1004“ auf Seite 439
- „nc.windows.gina.1005“ auf Seite 440
- „nc.windows.gina.1006“ auf Seite 440
- „nc.windows.gina.1007“ auf Seite 440
- „nc.windows.gina.1008“ auf Seite 440
- „nc.windows.gina.1009“ auf Seite 441
- „nc.windows.gina.1010“ auf Seite 441
- „nc.windows.gina.1011“ auf Seite 441
- „nc.windows.gina.1012“ auf Seite 441
- „nc.windows.gina.1013“ auf Seite 442
- „nc.windows.gina.1014“ auf Seite 442

nc.windows.app.1001

Systemprotokoll-meldung Die Ressource <*Ressourcenname*> kann nicht geladen werden. Stattdessen wird die englische Ressourcenbibliothek geladen.

Ursache Die angegebene Ressourcenbibliothek wurde nicht gefunden.

Aktion Installieren Sie den Network Connect-Client neu. Wenden Sie sich an Ihren Systemadministrator, wenn die gewünschte Ressource danach immer noch nicht verfügbar ist.

nc.windows.app.1002

Systemprotokoll-meldung Network Connect wird bereits auf diesem Client ausgeführt. Möchten Sie die aktuelle Sitzung beenden und eine neue Network Connect-Sitzung aufrufen?

Ursache Network Connect wird bereits auf diesem Computer ausgeführt.

Aktion Klicken Sie auf **Ja**, um die vorhandene Network Connect-Sitzung zu schließen und eine neue Sitzung zu starten. Klicken Sie auf **Nein**, um Network Connect zu schließen und die vorhandene Network Connect-Sitzung fortzusetzen.

nc.windows.app.1003

Systemprotokoll-meldung Der Treiber des virtuellen Adapters in Network Connect ist nicht korrekt installiert. Installieren Sie Network Connect neu.

Ursache Der Network Connect-Treiber ist nicht korrekt installiert.

Aktion Deinstallieren Sie Network Connect, installieren Sie die Anwendung neu, und versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Network Connect immer noch nicht korrekt installiert ist.

nc.windows.app.1004

Systemprotokoll-meldung Network Connect-Dienst kann nicht gestartet werden. Installieren Sie Network Connect neu.

Ursache Die Network Connect-Komponente NCService wird nicht ausgeführt, und der Client kann sie nicht starten.

Aktion Deinstallieren Sie Network Connect, installieren Sie die Anwendung neu, und versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie Network Connect auch jetzt nicht starten können.

nc.windows.app.1005

Systemprotokoll-meldung Die Network Connect-Komponente NCService wird nicht ausgeführt.

Ursache Der Network Connect-Dienst wird nicht ausgeführt, und der aktuelle Benutzer verfügt nicht über die erforderlichen Administratorrechte zum Starten des Dienstes.

Aktion Installieren Sie Network Connect neu, und versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie Network Connect auch jetzt nicht starten können.

nc.windows.app.1006

Systemprotokoll-meldung Möchten Sie die automatische Anmeldefunktion 'Graphical Identification and Authentication (GINA)' aktivieren, damit Network Connect beim Starten von Windows ebenfalls aufgerufen wird?

Ursache Der Systemadministrator hat die automatische GINA-Anmeldefunktion für Ihre Benutzerrolle aktiviert. Sie können GINA jetzt aktivieren oder zu einem späteren Zeitpunkt installieren. (GINA ermöglicht das Starten von Network Connect beim Start von Windows.)

Aktion Klicken Sie auf **Ja**, um die automatische GINA-Anmeldefunktion auf Ihrem Computer zu aktivieren. Klicken Sie auf **Nein**, um sich manuell an Network Connect anzumelden.

nc.windows.app.1007

Systemprotokoll-meldung Die automatische Anmeldefunktion „Graphical identification and Authentication (GINA)“ ist auf dem Computer aktiviert.

Ursache Der Systemadministrator hat die automatische GINA-Anmeldefunktion auf dem sicheren Gateway aktiviert. Network Connect wird daher beim Anmelden an Windows automatisch gestartet. Diese Funktion wird wirksam, wenn Sie Ihren Computer und Windows das nächste Mal starten.

Aktion Dies ist eine Informationsmeldung. Klicken Sie auf **OK**, um fortzufahren.

nc.windows.app.1008

Systemprotokoll-meldung Starten Sie zum Aktivieren der automatischen Verbindungsherstellung den Computer neu. Über die automatische Verbindungsherstellung können Sie beim Starten von Windows einen Network Connect-Tunnel aufrufen. Möchten Sie den Computer jetzt neu starten?

Ursache Der Benutzer hat im Optionsdialogfeld von Network Connect die Einstellung „Beim Anmelden an Windows Verbindung automatisch herstellen“ aktiviert. Diese Einstellung ist nur aktiviert, wenn der Administrator des sicheren Gateways dem Benutzer die Auswahl dieser Option auf dem Client erlaubt.

Aktion Klicken Sie auf **OK**, um den Computer neu zu starten und die automatische Verbindungsoption zu aktivieren. Klicken Sie auf **Nein**,wenn Sie den Computer später neu starten möchten. Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen, ohne die automatische Verbindungsoption zu aktivieren.

nc.windows.app.1009

Systemprotokoll-meldung Der Ordner APPDATA kann nicht geöffnet werden.

Ursache Der Ordner erfordert bestimmte Berechtigungen, ist nicht vorhanden, wurde gelöscht oder verschoben oder ist beschädigt.

Aktion Versuchen Sie, die Zugriffsebene des aktuellen Benutzers zu überprüfen, und vergewissern Sie sich, ob er seinen eigenen Anwendungsdatenordner öffnen kann. (Der Pfad des Ordners lautet APPDATA\Juniper Networks\Network Connect *<Version>*\.) Melden Sie sich anschließend von Network Connect ab, und melden Sie sich erneut an Windows an. Wenden Sie sich an Ihren Systemadministrator, wenn Sie den Anwendungsdatenordner immer noch nicht öffnen können.

nc.windows.app.1010

Systemprotokoll-meldung Daten wurden erfolgreich in Protokolldatei kopiert.

Ursache Diese Meldung bestätigt die erfolgreiche Aktualisierung der Protokolldatei.

Aktion Dies ist eine Informationsmeldung. Eine Aktion Ihrerseits ist nicht erforderlich.

nc.windows.app.1011

Systemprotokoll-meldung Verbindungsdaten können nicht angezeigt werden.

Ursache Network Connect kann Verbindungsinformationen des sicheren Gateways nicht abrufen und anzeigen. (Zu den Verbindungsinformationen zählen gesendete/empfangene Bytes, das Verschlüsselungsprotokoll sowie Informationen zur Komprimierung und zum Transportmodus.) Überprüfen Sie Ihre Firewall- oder Netzwerkkonfiguration, um sicherzustellen, dass der Client über eine Netzwerkverbindung mit dem sicheren Gateway verfügt.

Aktion Melden Sie sich vom sicheren Gateway ab, und versuchen Sie erneut, eine Verbindung herzustellen. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung herstellen können.

nc.windows.app.1012

Systemprotokoll-meldung Fehler bei der automatischen Verbindungsherstellung von Network Connect.

Ursache Network Connect kann die während der Windows-Anmeldung eingerichtete automatische Verbindung mit dem sicheren Gateway nicht herstellen.

Aktion Versuchen Sie nochmals, eine Verbindung mit dem sicheren Gateway herzustellen. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine automatische Verbindung mit dem sicheren Gateway herstellen können.

nc.windows.app.1013

Systemprotokoll-meldung Verbindung zum sicheren Gateway kann nicht hergestellt werden.

Ursache Network Connect kann keine Verbindung mit dem sicheren Gateway öffnen. Die wahrscheinliche Ursache ist ein Netzwerk- oder Firewallproblem oder ein Konfigurationsproblem im sicheren Gateway.

Aktion Überprüfen Sie gemeinsam mit dem Systemadministrator Ihre Netzwerkverbindung, die Proxyeinstellungen (sofern zutreffend) und die Firewall/Router-ACL-Regeln, um sicherzustellen, dass der Client eine Verbindung mit dem sicheren Gateway herstellen kann. Versuchen Sie dann nochmals, eine Verbindung mit dem sicheren Gateway herzustellen. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.windows.app.1014

Systemprotokoll-meldung Kann keine Verbindung zum sicheren Gateway herstellen.

Ursache Network Connect kann keine Verbindung mit dem sicheren Gateway herstellen. Die wahrscheinliche Ursache ist ein Netzwerk- oder Firewallproblem oder ein Konfigurationsproblem im sicheren Gateway.

Aktion Überprüfen Sie gemeinsam mit dem Systemadministrator Ihre Netzwerkverbindung, die Proxyeinstellungen (sofern zutreffend) und die Firewall/Router-ACL-Regeln, um sicherzustellen, dass der Client eine Verbindung mit dem sicheren Gateway herstellen kann. Versuchen Sie dann nochmals, eine Verbindung mit dem sicheren Gateway herzustellen. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.windows.app.1015

Systemprotokoll-meldung Verbindung zur NCService-Komponente kann nicht hergestellt werden.

Ursache Network Connect kann keine Verbindung mit der NCService-Komponente herstellen. Möglicherweise wurde der Network Connect-Dienst deaktiviert oder während der Network Connect-Installation ist ein Problem aufgetreten.

Aktion Starten Sie den Network Connect-Client neu. Wenn Sie keine Verbindung herstellen können, deinstallieren Sie Network Connect, installieren Sie die Anwendung neu, und wiederholen Sie die Anmeldung dann. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit der NCService-Komponente herstellen können.

nc.windows.app.1016

Systemprotokoll-meldung Verbindungsinformationen vom sicheren Gateway können nicht abgerufen werden.

Ursache Network Connect kann keine Informationen zur Verbindungskonfiguration vom sicheren Gateway abrufen. Die Verbindung mit dem IVE wurde möglicherweise unterbrochen.

Aktion Melden Sie sich vom sicheren Gateway ab, und versuchen Sie erneut, eine Verbindung herzustellen. Überprüfen Sie anschließend gemeinsam mit dem Systemadministrator Ihre Netzwerkverbindung, die Proxyeinstellungen (sofern zutreffend) und Firewall/Router-ACL-Regeln, um sicherzustellen, dass der Client eine Verbindung mit dem sicheren Gateway herstellen kann. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.windows.app.1017

Systemprotokoll-meldung Verbindungsinformationen vom sicheren Gateway können nicht abgerufen werden.

Ursache Network Connect hat eine Fehlermeldung empfangen, während Verbindungsinformationen vom sicheren Gateway abgerufen wurden. Das sichere Gateway ist unter Umständen nicht mehr erreichbar, oder es funktioniert nicht mehr einwandfrei.

Aktion Melden Sie sich vom sicheren Gateway ab, und versuchen Sie erneut, eine Verbindung herzustellen. (Sie können auch versuchen, das Problem durch Deinstallieren und anschließendes Neuinstallieren des Network Connect-Clients zu beheben.) Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung herstellen können.

nc.windows.app.1018

Systemprotokoll-meldung Für die Verbindung zum sicheren Gateway ist eine Proxyauthentifizierung erforderlich.

Ursache Zwischen Ihrem Client und dem sicheren Gateway ist ein Proxyserver konfiguriert. Dieser Proxyserver lässt Verbindungen mit dem sicheren Gateway nur zu, wenn gültige Authentifizierungsinformationen eingegeben werden.

Aktion Geben Sie gültige Anmeldeinformationen im Proxy-Authentifizierungsdialogfeld ein.

nc.windows.app.1019

Systemprotokoll-meldung Das Zeitlimit für die Network Connect-Sitzung wurde überschritten.

Ursache Der Network Connect-Client wurde aufgrund einer Überschreitung des Sitzungszeitlimits vom sicheren Gateway getrennt. Möglicherweise hat Ihre Sitzung das Leerlaufzeitlimit oder die vom Administrator im sicheren Gateway konfigurierte maximale Sitzungslänge überschritten.

Aktion Melden Sie sich am sicheren Gateway an, und starten Sie Network Connect erneut.

nc.windows.app.1020

Systemprotokoll-meldung Die Network Connect-Sitzung wurde beendet. Soll die Verbindung wiederhergestellt werden?

Ursache Der Network Connect-Client wurde aufgrund einer Änderung seiner Routingtabelle vom sicheren Gateway getrennt.

Aktion Klicken Sie auf **Ja**, um sich am sicheren Gateway anzumelden und Network Connect erneut zu starten. Klicken Sie auf **Nein**, um den Network Connect-Client zu schließen.

nc.windows.app.1021

Systemprotokoll-meldung Die Network Connect-Sitzung wurde beendet. Soll die Verbindung wiederhergestellt werden?

Ursache Der Network Connect-Client wurde aufgrund eines Fehlers in seiner Konfiguration vom sicheren Gateway getrennt. Möglicherweise ist ein Netzwerkadapter oder eine Hardwarekomponente ausgefallen.

Aktion Klicken Sie auf **Ja**, um die Verbindung mit dem sicheren Gateway erneut herzustellen. Klicken Sie auf **Nein**, um den Network Connect-Client zu schließen. Wenden Sie sich an den Systemadministrator, wenn weiterhin Probleme vorliegen, und überprüfen Sie die Systemkonfiguration Ihres Computers, bevor sich erneut am sicheren Gateway anmelden und Network Connect starten. Sie können auch versuchen, das Problem durch eine Deinstallation und Neuinstallation von Network Connect zu lösen.

nc.windows.app.1022

Systemprotokoll-meldung Das sichere Gateway verweigert die Verbindungsanforderung von diesem Client.

Ursache Das sichere Gateway hat die Verbindungsanforderung Ihres Computers verweigert.

Aktion Versuchen Sie nochmals, eine Verbindung mit dem sicheren Gateway herzustellen. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.windows.app.1023

Systemprotokoll-meldung Die Verbindung zum sicheren Gateway konnte nicht hergestellt werden.

Ursache Die vorherige Network Connect-Sitzung konnte nicht vom sicheren Gateway getrennt werden.

Aktion Vergewissern Sie sich, dass die vorherige Sitzung beendet ist, und versuchen Sie dann erneut, eine Verbindung mit dem sicheren Gateway herzustellen. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.windows.app.1024

Systemprotokoll-meldung Zeitüberschreitung: Die Network Connect-Sitzung wird wegen Inaktivität in <*x*> Minute(n) <*y*> Sekunde(n) beendet.

Ursache Ihre Network Connect-Sitzung war solange inaktiv, dass die automatische Beendigung eingeleitet wurde. Der Systemadministrator konfiguriert diesen Wert im sicheren Gateway.

Aktion Klicken Sie auf die Schaltfläche **Sitzung verlängern**, um Ihre Network Connect-Sitzung fortzusetzen.

nc.windows.app.1025

Systemprotokoll-meldung Zeitüberschreitung: Die Network Connect-Sitzung wird in <*x*> Minute(n) <*y*> Sekunde(n) beendet.

Ursache Ihre Network Connect-Sitzung nähert sich der vom Systemadministrator konfigurierten maximalen Sitzungsdauer.

Aktion Melden Sie sich nach der Beendigung der Sitzung am sicheren Gateway an, und starten Sie Network Connect erneut.

nc.windows.app.1026

Systemprotokoll-meldung Aufgrund von fehlenden Komponenten kann der Network Connect-Client nicht gestartet werden.

Ursache Die Anmeldedaten des eigenständigen Network Connect-Clients sind gültig, eine erforderliche Komponente fehlt jedoch. Network Connect muss die Sitzung beenden.

Aktion Deinstallieren Sie den eigenständigen Network Connect-Client, und installieren Sie ihn neu, bevor Sie Network Connect erneut starten.

nc.windows.app.1027

Systemprotokoll-meldung Der Systemadministrator von Network Connect hat die automatische Anmeldefunktion 'Graphical Identification and Authentication (GINA)' deaktiviert. Diese Änderung wird beim nächsten Windows-Start wirksam.

Ursache Die automatische GINA-Anmeldefunktion wurde ursprünglich für diesen Benutzer aktiviert, der Systemadministrator hat die Funktion aber auf dem sicheren Gateway deaktiviert.

Aktion Klicken Sie auf **OK**, um die Network Connect-Sitzung fortzusetzen.

nc.windows.app.1028

Systemprotokoll-meldung Zeitüberschreitung beim Versuch der Verbindungsherstellung

Ursache Für den Network Connect-Client ist eine Zeitüberschreitung aufgetreten, während er auf eine Antwort vom sicheren Gateway gewartet hat.

Aktion Schließen Sie den Network Connect-Client, und wiederholen Sie den Anmeldeversuch. Wenden Sie sich an den Systemadministrator, wenn Sie sich noch immer nicht anmelden können.

nc.windows.app.1029

Systemprotokoll-meldung Entsprechend der Konfiguration wird Network Connect zusammen mit Windows gestartet. Diese Funktion ist aufgrund von Konflikten mit anderen Windows-Anwendungen deaktiviert.

Ursache Der Systemadministrator hat die automatische GINA-Anmeldefunktion (Graphical Identification and Authentication) für diese Benutzerrolle auf dem sicheren Gateway aktiviert, auf ihrem Computer ist jedoch eine vorhandene GINA-Komponente von einer anderen Anwendung installiert.

Aktion Klicken Sie auf **OK**, um fortzufahren. Melden Sie sich nach der Anmeldung an Windows am sicheren Gateway an, und starten Sie Network Connect über die Webkonsolenseite des sicheren Gateways.

nc.windows.app.1030

Systemprotokoll-meldung Sie können Network Connect nur mit Administratorberechtigungen auf diesem Computer installieren. Die Network Connect-Installation wurde abgebrochen.

Ursache Der zurzeit an diesem Computer angemeldete Benutzer besitzt keine Administratorrechte. Zum Installieren und Ausführen des Network Connect-Clients sind diese Rechte erforderlich.

Aktion Melden Sie sich als Systemadministrator an Windows an, und versuchen Sie erneut, Network Connect zu installieren.

nc.windows.app.1031

Systemprotokoll-meldung Network Connect wird nicht auf diesem Betriebssystem unterstützt. Die Network Connect-Installation wurde abgebrochen.

Ursache Nur Windows 2000 und Windows XP unterstützen die Installation dieser Version des Network Connect-Clients.

Aktion Klicken Sie auf **OK**, um die Installation von Network Connect zu beenden.

nc.windows.app.1032

Systemprotokoll-meldung Entsprechend der Konfiguration wird Network Connect zusammen mit Windows gestartet. Diese Funktion ist aufgrund von Konflikten mit anderen Windows-Anwendungen deaktiviert. Die Network Connect-Installation wurde abgebrochen.

Ursache Der Systemadministrator hat die automatische GINA-Anmeldefunktion (Graphical Identification and Authentication) für diese Benutzerrolle auf dem sicheren Gateway aktiviert, auf ihrem Computer ist jedoch eine vorhandene GINA-Komponente von einer anderen Anwendung installiert.

Aktion Klicken Sie auf **OK**, um die Installation zu beenden. Melden Sie sich nach der Anmeldung an Windows am sicheren Gateway an, und starten Sie Network Connect über die Webkonsolenseite des sicheren Gateways.

nc.windows.app.1033

Systemprotokoll-meldung Fehler bei der Network Connect-Aktualisierung. Deinstallieren Sie Network Connect manuell, und führen Sie das Installationsprogramm erneut aus.

Ursache Bei der Network Connect-Aktualisierung ist ein Problem aufgetreten. Network Connect wurde möglicherweise teilweise installiert, wodurch der Deinstallationsschritt im Aktualisierungsprozess fehlschlägt.

Aktion Schließen Sie diese Meldung mit **OK**, deinstallieren Sie Network Connect manuell, und installieren Sie dann die aktualisierte Version.

nc.windows.app.1034

Systemprotokoll-meldung Sie müssen zum Abschließen der Network Connect-Installation den Computer neu starten. Möchten Sie den Computer jetzt neu starten?

Ursache Bei der Network Connect-Installation ist ein Problem aufgetreten. Die vorherige Version der NCService-Komponente wurde möglicherweise nicht im Dienststeuerungs-Manager beendet.

Aktion Klicken Sie auf **Ja**, um die Aktualisierung abzuschließen und den Computer neu zu starten.

nc.windows.app.1035

Systemprotokoll-meldung Zum Abschließen der Einrichtung von Network Connect müssen Sie den Computer neu starten.

Ursache Im Deinstallationsschritt des Network Connect-Setups ist ein Fehler beim Beenden der NCService-Komponente aufgetreten. Sie müssen den Computer zum Beheben des Problems neu starten.

Aktion Klicken Sie auf **OK**, um den Computer neu zu starten und die Network Connect-Installation abzuschließen.

nc.windows.app.1036

Systemprotokoll-meldung Sie können Network Connect nur mit Administratorberechtigungen auf diesem Computer deinstallieren. Die Network Connect-Einrichtung wurde abgebrochen.

Ursache Sie besitzen keine Administratorberechtigungen.

Aktion Wenden Sie sich an den Systemadministrator.

nc.windows.app.1037

Systemprotokoll-meldung Network Connect wird bereits auf diesem Client ausgeführt. Beenden Sie die vorhandene Sitzung, bevor Sie eine neue Sitzung starten.

Ursache Network Connect wird bereits auf diesem Computer ausgeführt.

Aktion Klicken Sie auf **OK**, um die neue Network Connect-Anwendung zu schließen, beenden Sie manuell die vorhandene Network Connect-Sitzung, und starten Sie Network Connect erneut.

nc.windows.app.1038

Systemprotokoll-meldung Network Connect konnte die automatische Anmeldefunktion 'Graphical Identification and Authentication (GINA)' nicht initialisieren.

Ursache Entweder besitzen Sie keine entsprechenden Administratorrechte, oder der Juniper Installer Service ist nicht auf diesem Computer installiert.

Aktion Bitten Sie den Systemadministrator, den Juniper Installer Service oder die korrekte GINA-fähige Network Connect-Anwendung auf dem Computer zu installieren.

nc.windows.app.1039

Systemprotokoll-meldung Network Connect konnte die automatische Anmeldefunktion 'Graphical Identification and Authentication (GINA)' nicht deaktivieren.

Ursache Der Systemadministrator hat GINA für Ihre Benutzerrolle deaktiviert. Entweder besitzen Sie jedoch keine entsprechenden Administratorrechte, oder der Juniper Installer Service ist nicht auf diesem Computer installiert.

Aktion Bitten Sie den Systemadministrator, den Juniper Installer Service oder die korrekte Network Connect-Anwendung auf dem Computer zu installieren.

nc.windows.app.1040

Systemprotokoll-meldung Network Connect hat festgestellt, dass auf Ihrem Computer Plug&Play deaktiviert ist. Ihr System lässt derzeit nicht zu, dass bestimmte Komponenten von Network Connect auf Ihrem Computer installiert werden. Schlagen Sie in der Onlinedokumentation zum sicheren Gateway Anweisungen zum Aktivieren von Plug&Play nach.

Ursache Diese Meldung wird angezeigt, wenn Plug&Play von einer anderen Anwendung auf dem Computer deaktiviert wurde. Dadurch wird die vollständige Installation des Network Connect-Treibers verhindert.

Aktion Der folgende Registrierungsschlüssel sollte auf dem Clientsystem erstellt werden: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce. Dadurch wird Plug&Play auf dem Clientsystem aktiviert.

nc.windows.gina.1001

Systemprotokoll-meldung Die Network Connect-Anmeldung über die automatische Anmeldefunktion 'Graphical Identification and Authentication (GINA)' ist nicht auf dem sicheren Gateway konfiguriert.

Ursache Die Anmeldedaten des Benutzers sind gültig, der Systemadministrator hat jedoch GINA nicht für die Rolle des Benutzers aktiviert.

Aktion Wenden Sie sich an den Systemadministrator, um sicherzustellen, dass GINA für die Rolle des Benutzers aktiviert ist.

nc.windows.gina.1002

Systemprotokoll-meldung Network Connect-Tunnel konnte nicht eingerichtet werden. Die automatische Anmeldefunktion 'Graphical identification and Authentication (GINA)' ist auf dem sicheren Gateway deaktiviert.

Ursache Die Anmeldedaten des Benutzers sind gültig, GINA ist jedoch nicht für die Rolle des Benutzers aktiviert. GINA wurde möglicherweise in einer vorherigen Installation für diese Rolle aktiviert und dann vom Systemadministrator deaktiviert.

Aktion Wenden Sie sich an den Systemadministrator, um sicherzustellen, dass GINA für die Rolle des Benutzers aktiviert ist.

nc.windows.gina.1003

Systemprotokoll-meldung Kein Authentifizierungszertifikat gefunden. Möchten Sie sich trotzdem beim sicheren Gateway anmelden?

Ursache Das erforderliche MD5-Zertifikat konnte nicht auf dem Computer des Benutzers gefunden werden. Sie haben sich zuvor möglicherweise nicht mit diesem Webbrowser am sicheren Gateway angemeldet.

Aktion Klicken Sie auf **OK**, um die MD5-Zertifikatauthentifizierung zu aktivieren und sich am sicheren Gateway anzumelden. Klicken Sie auf **Abbrechen**, um die Anmeldung an Network Connect abzubrechen.

nc.windows.gina.1004

Systemprotokoll-meldung Authentifizierung des sicheren Gateways fehlgeschlagen.

Ursache Der für die Authentifizierung eingegebene Benutzername und/oder das Kennwort sind ungültig und wurden vom sicheren Gateway abgelehnt.

Aktion Überprüfen Sie den Benutzernamen und das Kennwort, und wiederholen Sie den Anmeldeversuch. Wenden Sie sich an den Systemadministrator, wenn Sie der Meinung sind, dass der Benutzername und das Kennwort korrekt sind.

nc.windows.gina.1005

Systemprotokoll-meldung Network Connect-Tunnel konnte nicht eingerichtet werden.

Ursache Ein Network Connect-Tunnel zwischen dem Client und dem sicheren Gateway konnte nicht eingerichtet werden. Die Verbindung im Netzwerk ist u. U. vorübergehend ausgefallen. Möglicherweise liegt ein Problem mit den Proxyeinstellungen vor, oder zwischen der automatischen GINA-Anmeldefunktion (Graphical Identification and Authentication) und dem Network Connect-Dienst liegt ein Kommunikationsfehler vor.

Aktion Bitten Sie den Systemadministrator, die Netzwerkverbindung, die Proxyeinstellungen und die Einstellungen des sicheren Gateways zu überprüfen.

nc.windows.gina.1006

Systemprotokoll-meldung Die Verbindung zum sicheren Gateway wurde getrennt.

Ursache Der Network Connect-Dienst wurde während der Authentifizierung unerwartet beendet.

Aktion Melden Sie sich an Windows, und deinstallieren Sie Network Connect. Melden Sie sich dann am sicheren Gateway an, und installieren Sie Network Connect neu.

nc.windows.gina.1007

Systemprotokoll-meldung Network Connect-Tunnel konnte nicht eingerichtet werden. Sie sind auf dem sicheren Gateway mit mehreren Benutzerrollen verknüpft. Dies ist nicht kompatibel mit der automatischen Anmeldefunktion 'Graphical Identification and Authentication (GINA)'.

Ursache Das sichere Gateway ist zur Anzeige einer Rollenauswahlseite für den Benutzer konfiguriert. Diese Funktion wird nicht unterstützt, wenn GINA für die Rolle des Benutzers aktiviert ist.

Aktion Der Systemadministrator muss sicherstellen, dass GINA für den Benutzer deaktiviert oder der Benutzer nur einer Rolle zugeordnet ist.

nc.windows.gina.1008

Systemprotokoll-meldung In zwei aufeinander folgenden Versuchen konnte das sichere Gateway Ihre Anmeldeinformationen nicht authentifizieren. Die automatische Anmeldefunktion 'Graphical Identification and Authentication (GINA)' wird während der aktuellen Windows-Anmeldesitzung keine weiteren Anmeldeversuche am sicheren Gateway vornehmen.

Ursache In zwei aufeinander folgenden Versuchen konnte das sichere Gateway die angegebenen Anmeldeinformationen nicht authentifizieren.

Aktion Überprüfen Sie Ihre Anmeldedaten, und stellen Sie nach dem Start von Windows eine Verbindung mit dem sicheren Gateway her. Wenden Sie sich an den Systemadministrator, wenn Sie der Meinung sind, dass die während der Windows-Anmeldung verwendeten Anmeldedaten korrekt waren.

nc.windows.gina.1009

Systemprotokoll-meldung Die Verbindung zum Network Connect-Tunnel wurde getrennt, da der Benutzer weder bei Windows NT noch an der Windows Active Directory-Domäne angemeldet ist.

Ursache Möglicherweise haben Sie sich mit zwischengespeicherten Anmeldedaten an der Windows-Sitzung angemeldet, die nicht mit den Anmeldedaten für die Windows NT- oder Windows Active Directory-Domäne übereinstimmen.

Aktion Vergewissern Sie sich, dass Ihr Computer ein Mitglied der korrekten Windows NT- oder Windows Active Directory-Domäne ist und Ihre Windows-Anmeldedaten gültig sind.

nc.windows.gina.1010

Systemprotokoll-meldung Geben Sie eine gültige Proxyserver-IP-Adresse oder einen gültigen Hostnamen ein.

Ursache Die Proxyserveroption wurde aktiviert, die Proxy-IP-Adresse oder der Hostname ist jedoch ungültig, oder es wurden keine gültigen Proxyserverinformationen angegeben.

Aktion Stellen Sie sicher, dass die Proxyserverinformationen gültig sind, und versuchen Sie erneut, sich am sicheren Gateway anzumelden.

nc.windows.gina.1011

Systemprotokoll-meldung Geben Sie den kompletten URL im Format https://www.server.ihrefirma.de an.

Ursache Der eingegebene URL ist ungültig oder falsch formatiert.

Aktion Stellen Sie sicher, dass der URL das Präfix „https://“ enthält und der Hostname des sicheren Gateways korrekt ist.

nc.windows.gina.1012

Systemprotokoll-meldung Geben Sie den für die Kommunikation mit dem Proxyserver erforderlichen HTTP-Port ein.

Ursache Der für den Proxyserver angegebene Port ist falsch oder kein TCP-Port.

Aktion Bitten Sie den Systemadministrator, die Portnummer für den Proxyserver zu überprüfen.

nc.windows.gina.1013

Systemprotokoll-meldung Geben Sie einen vom sicheren Gateway erkannten Benutzernamen ein.

Ursache Das Benutzernamenfeld wurde nicht ausgefüllt.

Aktion Geben Sie einen gültigen Benutzernamen ein, und wiederholen Sie den Verbindungsversuch.

nc.windows.gina.1014

Systemprotokoll-meldung Die aktuelle Version von Network Connect kann mit der Funktion Graphical Identification and Authentication (GINA) zur automatischen Anmeldung nicht gestartet werden. Die von Ihnen ausgeführte Version ist älter als die Version auf dem sicheren Gateway. Melden Sie sich nach dem Starten von Windows am sicheren Gateway an, und aktualisieren Sie Ihre Version von Network Connect.

Ursache Die von Ihnen ausgeführte Version von Network Connect ist älter als die Version auf dem sicheren Gateway. Daher kann die automatische GINA-Anmeldefunktion Network Connect beim Start von Windows nicht starten.

Aktion Melden Sie sich nach dem Starten von Windows am sicheren Gateway an, und aktualisieren Sie Ihre Version von Network Connect.

Macintosh-Fehlermeldungen

Dieser Abschnitt behandelt Network Connect-Fehlermeldungen für Macintosh:

- „nc.mac.app.1003“ auf Seite 443
- „nc.mac.app.1004“ auf Seite 443
- „nc.mac.app.1005“ auf Seite 443
- „nc.mac.app.1100“ auf Seite 444
- „nc.mac.app.1104“ auf Seite 444
- „nc.mac.app.1106“ auf Seite 444
- „nc.mac.app.1108“ auf Seite 444
- „nc.mac.app.1109“ auf Seite 445
- „nc.mac.app.1200“ auf Seite 445
- „nc.mac.app.1202“ auf Seite 445
- „nc.mac.app.1203“ auf Seite 446
- „nc.mac.app.1204“ auf Seite 446
- „nc.mac.app.1205“ auf Seite 446

- „nc.mac.app.1206“ auf Seite 446
- „nc.mac.app.1207“ auf Seite 447
- „nc.mac.app.1400“ auf Seite 447
- „nc.mac.app.1401“ auf Seite 447
- „nc.mac.app.1402“ auf Seite 447
- „nc.mac.app.1403“ auf Seite 448
- „nc.mac.app.1700“ auf Seite 448
- „nc.mac.app.1701“ auf Seite 448
- „nc.mac.app.1804“ auf Seite 448
- „nc.mac.app.1805“ auf Seite 449

nc.mac.app.1003

Systemprotokoll-meldung Network Connect kann keine Verbindung zum sicheren Gateway herstellen.

Ursache Das sichere Gateway verwendet den eigenständigen Network Connect-Client, die Verbindung wurde jedoch abgelehnt, oder das Zeitlimit wurde überschritten.

Aktion Stellen Sie sicher, dass Sie den Hostnamen oder die IP-Adresse richtig eingegeben haben, und versuchen Sie dann nochmals, sich am sicheren Gateway anzumelden.

nc.mac.app.1004

Systemprotokoll-meldung Network Connect kann das sichere Gateway nicht finden.

Ursache Das sichere Gateway kann mit dem eigenständigen Network Connect-Client nicht gefunden werden. Möglicherweise haben Sie einen falschen Hostnamen eingegeben, oder es liegt ein DNS-Konfigurationsproblem vor.

Aktion Stellen Sie sicher, dass Sie den Hostnamen oder die IP-Adresse richtig eingegeben haben, und versuchen Sie dann nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1005

Systemprotokoll-meldung Network Connect kann keine Verbindung zum sicheren Gateway herstellen.

Ursache Der eigenständige Network Connect-Client konnte die erforderlichen Daten nicht vom sicheren Gateway abrufen. Das sichere Gateway hat möglicherweise eine Ressource mit Null Byte für eine Funktion „HTTPS GET“ auf der ersten Seite zurückgegeben. Dies kann bei Verwendung eines nicht korrekt konfigurierten HTTPS-Proxy passieren. In diesem Fall zeigt Safari eine leere Seite für alle durch den Proxy geleiteten Sitzungsinformationen an.

Aktion Versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1100

Systemprotokoll-meldung Network Connect wird bereits ausgeführt.

Ursache Es wird bereits eine andere Instanz von Network Connect auf Ihrem Computer ausgeführt. Sie können jeweils nur eine Network Connect-Sitzung auf dem Computer starten.

Aktion Vergewissern Sie sich vor dem Start von Network Connect, dass keine anderen Network Connect-Sitzungen ausgeführt werden.

nc.mac.app.1104

Systemprotokoll-meldung Das Zeitlimit für die Sitzung wurde überschritten.

Ursache Die Sitzung wurde beendet, weil Network Connect mindestens 90 Sekunden lang keine Takt-/Überprüfungsmeldung vom sicheren Gateway empfangen hat. (Weitere Informationen finden Sie in der Protokollanzeige.)

Aktion Melden Sie sich erneut am sicheren Gateway an. Wenden Sie sich an Ihren Systemadministrator, wenn Sie keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1106

Systemprotokoll-meldung Möchten Sie Network Connect aktualisieren?

Ursache Die Version des eigenständigen Network Connect-Clients auf Ihrem Computer (<*Version*>) stimmt nicht mit der Version im sicheren Gateway (<*Version*>) überein.

Aktion Klicken Sie auf **Aktualisieren**, um Ihre Version von Network Connect zu aktualisieren, oder klicken Sie auf **Abbrechen**, um die Verbindung zu beenden.

nc.mac.app.1108

Systemprotokoll-meldung Die Netzwerkschnittstelle Ihres Computers hat sich geändert.

Ursache Die Netzwerkeinstellungen Ihres Computers haben sich unabhängig von der Network Connect-Sitzung geändert. Entsprechend den auf dem sicheren Gateway konfigurierten Sicherheitsrichtlinien wurde die Verbindung getrennt. Folgendes kommt hierfür als Ursache in Frage: Änderungen an den Systemeinstellungen, Aktivierung oder Ausfall von Netzwerkschnittstellen (z. B., PPP, AirPort Wireless), Erneuerung einer DHCP-Leihdauer oder Eindringen eines böswilligen Agenten in das System.

Aktion Klicken Sie auf **Verbindung wieder herstellen**, um die Network Connect-Sitzung wieder herzustellen, oder klicken Sie auf **Abbrechen**. Bei Verwendung eines eigenständigen Clients wird das Anmeldefenster von Network Connect angezeigt. Wenn Sie einen über das Web gestarteten Client verwenden, wird das Programm beendet.

nc.mac.app.1109

Systemprotokoll-meldung Die Netzwerkschnittstelle Ihres Computers hat sich geändert.

Ursache Die Netzwerkeinstellungen Ihres Computers haben sich unabhängig von der Network Connect-Sitzung geändert. Entsprechend den auf dem sicheren Gateway konfigurierten Sicherheitsrichtlinien wurde die Verbindung getrennt. Folgendes kommt hierfür als Ursache in Frage: Änderungen an den Systemeinstellungen, Aktivierung oder Ausfall von Netzwerkschnittstellen (z. B., PPP, AirPort Wireless), Erneuerung einer DHCP-Leihdauer oder Eindringen eines böswilligen Agenten in das System.

Aktion Klicken Sie auf **OK**. Bei Verwendung eines eigenständigen Clients wird das Anmeldefenster von Network Connect angezeigt. Wenn Sie einen über das Web gestarteten Client verwenden, wird das Programm beendet.

nc.mac.app.1200

Systemprotokoll-meldung Network Connect kann keine sichere Sitzung aufrufen.

Ursache Network Connect kann den Tunneling-Dienst nicht starten. Möglicherweise ist während der Installation ein Problem aufgetreten. (Weitere Informationen finden Sie in der Protokollanzeige.)

Aktion Installieren Sie Network Connect neu, und versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1202

Systemprotokoll-meldung Network Connect kann keine sichere Sitzung aufrufen.

Ursache Network Connect konnte die Kommunikation mit dem sicheren Gateway starten, aus einem unbekannten Grund konnte jedoch der Tunneling-Dienst nicht gestartet werden. (Weitere Informationen finden Sie in der Protokollanzeige.)

Aktion Installieren Sie Network Connect neu, und versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1203

Systemprotokoll-meldung Die Sitzung wurde plötzlich abgebrochen.

Ursache Der Tunneling-Dienst von Network Connect wurde aufgrund eines Softwarefehlers beendet. Dies kann auf einen Beendigungscode ungleich Null zurückzuführen sein (ein solcher Code ist normalerweise ein Indiz für einen Softwareabsturz). (Weitere Informationen finden Sie in der Protokollanzeige.)

Aktion Versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1204

Systemprotokoll-meldung Die Routingtabelle Ihres Computers hat sich geändert.

Ursache Die Routingtabelle Ihres Computers wurde unabhängig von Network Connect geändert. Entsprechend den auf dem sicheren Gateway konfigurierten Sicherheitsrichtlinien wurde die Verbindung getrennt.

Aktion Klicken Sie auf **Verbindung wieder herstellen**, um die Network Connect-Sitzung wieder herzustellen, oder klicken Sie auf **Abbrechen**. Bei Verwendung eines eigenständigen Clients wird das Anmeldefenster von Network Connect angezeigt. Wenn Sie einen über das Web gestarteten Client verwenden, wird das Programm beendet.

nc.mac.app.1205

Systemprotokoll-meldung Die Routingtabelle Ihres Computers hat sich geändert.

Ursache Die Routingtabelle Ihres Computers wurde unabhängig von Network Connect geändert. Entsprechend den auf dem sicheren Gateway konfigurierten Sicherheitsrichtlinien wurde die Verbindung getrennt.

Aktion Klicken Sie auf **OK**. Bei Verwendung eines eigenständigen Clients wird das Anmeldefenster von Network Connect angezeigt. Wenn Sie einen über das Web gestarteten Client verwenden, wird das Programm beendet.

nc.mac.app.1206

Systemprotokoll-meldung Network Connect kann keine sichere Sitzung aufrufen.

Ursache Der Tunneling-Dienst von Network Connect kann über diesen HTTPS-Proxyserver keine Authentifizierung durchführen. (Weitere Informationen finden Sie in der Protokollanzeige.)

Aktion Versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1207

Systemprotokoll-meldung Das Zeitlimit für die Sitzung wurde überschritten.

Ursache Ihre Network Connect-Sitzung ist aufgrund der im sicheren Gateway konfigurierten Beschränkung der Sitzungsdauer abgelaufen.

Aktion Versuchen Sie nochmals, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1400

Systemprotokoll-meldung Network Connect konnte den HTTPS-Proxy nicht verwenden.

Ursache Das PAC-Skript (Automatic Proxy Configuration) konnte nicht über den unter „Netzwerk“ auf der Seite „Systemeinstellungen“ angegebenen URL geladen werden. Möglicherweise ist die im Textfeld in den Systemeinstellungen eingegebene Zeichenfolge kein URL.

Aktion Überprüfen Sie in den Systemeinstellungen den URL für das PAC-Skript, und versuchen Sie erneut, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1401

Systemprotokoll-meldung Network Connect konnte den HTTPS-Proxy nicht verwenden.

Ursache Das PAC-Skript (Automatic Proxy Configuration) konnte nicht über den unter „Netzwerk“ auf der Seite „Systemeinstellungen“ angegebenen URL geladen werden. Dies kann auf einen DNS-Fehler (Domain Name Service) oder einen Netzwerkverbindungsfehler zurückzuführen sein.

Aktion Überprüfen Sie in den Systemeinstellungen den URL für das PAC-Skript, und versuchen Sie erneut, sich am sicheren Gateway anzumelden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie immer noch keine Verbindung mit dem sicheren Gateway herstellen können.

nc.mac.app.1402

Systemprotokoll-meldung Network Connect konnte den HTTPS-Proxy nicht verwenden.

Ursache Das PAC-Skript (Automatic Proxy Configuration) unter dem im Bereich „Netzwerk“ der Seite „Systemeinstellungen“ angegebenen URL enthält möglicherweise Fehler. Wenn dies nicht der Fall ist, ist die PAC-Datei unter Umständen keine Textdatei, oder sie verwendet eine nicht als UTF-8 lesbare Verschlüsselungsmethode.

Aktion Wenden Sie sich an Ihren Netzwerkadministrator, und versuchen Sie nochmals, sich am sicheren Gateway anzumelden.

nc.mac.app.1403

Systemprotokoll-meldung Network Connect konnte den HTTPS-Proxy nicht verwenden.

Ursache Das PAC-Skript (Automatic Proxy Configuration) unter dem im Bereich „Netzwerk“ der Seite „Systemeinstellungen“ angegebenen URL enthält möglicherweise Fehler. Das PAC-Skript enthält unter Umständen Syntaxfehler.

Aktion Wenden Sie sich an Ihren Netzwerkadministrator, und versuchen Sie nochmals, sich am sicheren Gateway anzumelden.

nc.mac.app.1700

Systemprotokoll-meldung Die Deinstallation von Network Connect ist fehlgeschlagen.

Ursache Bei der Deinstallation von Network Connect ist ein Fehler aufgetreten.

Aktion Wenden Sie sich an Ihren Netzwerkadministrator, bevor Sie Network Connect deinstallieren oder sich erneut am sicheren Gateway anmelden.

nc.mac.app.1701

Systemprotokoll-meldung Fehler bei der Network Connect-Aktualisierung.

Ursache Das eigenständige Network Connect-Aktualisierungspaket konnte aufgrund eines Netzwerkfehlers nicht heruntergeladen werden.

Aktion Wenden Sie sich an Ihren Netzwerkadministrator, bevor Sie Network Connect erneut installieren.

nc.mac.app.1804

Systemprotokoll-meldung Ihre Sitzung wird in Kürze beendet.

Ursache Wenn der Zeitgeber Null erreicht, wird Ihre Sitzung aufgrund der im sicheren Gateway konfigurierten Längenbeschränkungen beendet.

Aktion Klicken Sie auf **OK**. Starten Sie Network Connect nach der Beendigung der Sitzung, oder melden Sie sich erneut am sicheren Gateway an.

nc.mac.app.1805

Systemprotokoll-meldung Möchten Sie die Sitzung verlängern?

Ursache Sie nähern sich dem im sicheren Gateway konfigurierten maximalen Leerlaufzeitlimit für Sitzungen. Wenn Sie die Network Connect-Sitzung nicht verlängern, wird die Sitzung aufgrund von Inaktivität beendet, sobald der Zeitgeber Null erreicht.

Aktion Klicken Sie auf **Sitzung verlängern**, um die Sitzung zu verlängern, klicken Sie auf **Abmelden**, um die Verbindung mit dem sicheren Gateway zu beenden, oder klicken Sie auf **Keine Aktion**, um die Verbindung ablaufen zu lassen, wenn der Zeitgeber Null erreicht.

Index

Ziffern

128-Bit-Verschlüsselung 165
168-Bit-Verschlüsselung 165

A

Ablaufverfolgungsdatei (zum Debuggen) 381
Access Series, Definition 37
Access-Accept-Authentifizierung 238
Access-Challenge-Authentifizierung 238
Access-Reject-Authentifizierung 238
Access-Request-Authentifizierung 238
ACE *siehe* RSA ACE
Active Directory
    Siehe Authentifizierungsserver, Active Directory
Administrator
    Benutzeradministrator 223
    Superadministrator-Konto erstellen 396
Administratorbereiche 367
Administratorrolle
    Definition 56, 267
    siehe auch Rolle
Advanced Preferences
    siehe Benutzer
AES-Verschlüsselung, Unterstützung 235
Aktion, Bestandteil einer Ressourcenrichtlinie 60
Aktive Benutzer überwachen 156
Aktualisieren des IVE 360
Anmeldeinformationen
    Überprüfung 35
    Windows 335
Anmelderichtlinien
    aktivieren 204
    deaktivieren 204
    Definition 36, 55, 203
    konfigurieren 203
    vorkonfigurierte Richtlinien 36
Anmeldeseiten 367
    Definition 55, 204
    Zuordnung zu Anmelderichtlinien 203
Anmelde-URLs 367
Anmeldung
    Optionen
        Benutzereinschränkungen 418, 419, 421, 422, 423, 425
Antivirensoftware
    Anforderungen angeben 74
    auf aktuelle Versionen prüfen 212
Anwendungscaches leeren 75, 87
Applet
    Browsingoption konfigurieren 288
archiveFileTransferFailed, MIB-Objekt 198
archiveServerLoginFailed, MIB-Objekt 197
archiveServerUnreachable, MIB-Objekt 197
Archivierung
    Definition 127
    Planung 376
ARP Ping Timeout, Konfiguration 187, 189
ARP-Befehl 383, 384, 395
ARP-Cache, Konfiguration 124, 188, 189
Attribute
    XML 136
Attribute konfigurieren 261
Attributserver
    siehe Authentifizierungsserver
Aufzeichnen von Benutzersitzungen 378
Authentifizierung
    unterstützte Server 52
Authentifizierungsbereiche
    siehe Bereich
Authentifizierungseinstellungen
    für Benutzer 418, 421, 422, 423, 425
Authentifizierungsrichtlinien
    Definition 36, 38, 51
    konfigurieren 53, 260
Authentifizierungsserver
    ACE/Server
        ACE/Agent-Datei generieren 236
        Agent-Konfigurationsdatei 236
        konfigurieren 235
        Übersicht 234
    Active Directory
        konfigurieren 223, 245
    anonymer Server
        konfigurieren 251, 254
        Übersicht 250
    Definition 35, 38, 51
    einem Bereich zuordnen 257
    Konfiguration (grundlegende Schritte) 224
    LDAP
        Attribute konfigurieren 261
        konfigurieren 223, 230
    lokale Authentifizierung 225
        konfigurieren 224, 254

NIS-Server
konfigurieren ... 233
RADIUS ... 238
ACE/Server-Protokoll ... 235
Attribute konfigurieren ... 261
Verzeichnisserver, Definition ... 38
vorkonfigurierte Server ... 35
Zertifikatserver
Definition ... 67
konfigurieren ... 252
LDAP
Authentifizierung mit 253
authServerName MIB-Objekt ... 195
Auto-allow
Lesezeichen, Datei ... 293
Lesezeichen, Web ... 285
Autorisierungsserver
siehe Authentifizierungsserver

B

Basis-CRL
Definition ... 69
siehe auch Zertifikatsperrlisten
Befehle, UNIX ... 383, 384
Benutzerbereiche
exportieren ... 367
Benutzerdefinierte NHC-Integration
siehe Host Checker-API
Benutzerkonten
exportieren ... 368
lokal ... 368
Benutzer
Rolle
siehe auch Rolle
Benutzerrolle
siehe Rolle
Benutzersitzung
siehe Sitzung
Bereich
Definition ... 36, 38
konfigurieren ... 257, 417
Sicherheitsanforderungen ... 39
vorkonfigurierte Bereiche ... 36
Zuordnung zu Anmelderichtlinie ... 203
Bereiche
exportieren ... 367
blockedIP MIB-Objekt ... 195
blockedIPList MIB-Objekt ... 196
Browser
Anmeldeeinschränkungen, Benutzer ... 419
Einschränkungen konfigurieren ... 47
Browsing
Optionen für das Web festlegen ... 288
Optionen für die Datei festlegen ... 295
Seite öffnen ... 289
Browsingprobleme (Web) ... 381

C

Cache
Header ... 314
Java-Plug-In ... 73
leeren ... 75, 87
Regeln ... 312
Cache Cleaner
Protokollierung deaktivieren ... 199
Übersicht ... 87
Cache-Control
No-Store ... 314
CASQUE-Authentifizierung ... 243
cHTML
Kennwörter maskieren ... 185
Seiten aktivieren ... 184
Clientseitige Java-Applets
Verbindungen angeben ... 316, 318, 319
Cluster
ACE/Server-Unterstützung ... 235
clusterConcurrentUsers MIB-Objekt ... 196
Codesignaturrichtlinien für Java ... 317
Codesignaturzertifikat
siehe Zertifikat, Appletzertifikat
Codierung von Ressourcenrichtlinien ... 339
Compact HTML
Maskieren von Kennwörtern ... 185
Compact HTML-Seiten
aktivieren ... 184
Cookies
löschen beim Abbruch der Sitzung ... 165
permanente, aktivieren ... 290
cpuUtilNotify MIB-Objekt ... 198
Critical (Protokollmeldung), Definition ... 127
CRL ... 35
siehe Zertifikat, Sperrliste
CyberGatekeeper
erzwingen ... 208
Integration ... 76

D

Datei
Lesezeichen erstellen ... 293, 294
Prüfung
konfigurieren ... 210
Übersicht ... 74, 77
Ressourcenrichtlinien ... 332
Definition ... 333, 334
Server, Codierung ... 339
Zugriffsstatistik ... 199
Dateibereinigung ... 75, 87
Datenbank für Authentifizierung ... 52
Datum und Uhrzeit einstellen ... 155
Debugging
Ablaufverfolgungsdatei ... 381
remote ... 384
Snapshotdatei ... 382
TCP-Dumpdatei ... 382
UNIX-Befehle ... 383, 384

delegierte Administratorrollen
exportieren....368
DES/SDI-Verschlüsselung, Unterstützung....235
Dienstpaket
herunterladen....155
installieren....360
Digitales Zertifikat
Definition....65
Siehe auch Zertifikat
siehe Zertifikat
diskFullPercent MIB-Objekt....196
Distinguished Name-Attribute, Angabe....179
DLL-Anforderungen, Host Checker
siehe Host Checker
Clientschnittstelle
Server-Integrationsschnittstelle
DMZ
Schnittstelle....187, 188
DN-Attribute, Angabe....179
DNS
für externen Port....187, 188
Hostname, Definition in Ressourcenrichtlinien 305, 309
Namensauflösung, Konfiguration....186
Durchgangsproxy
Anwendungen angeben für....321
Beschreibung....117
Ressourcenrichtlinien....322
dynamische Richtlinienauswertung....44, 78, 207, 258

E

Einschränkungen
Benutzeranmeldung....421, 422
Elemente
Instanz....133
E-Mail-Client
konfigurieren....354
MIB-Objekt....195
Ressourcenrichtlinien
Übersicht....106
Ende-Tag
XML....134
Endpoint Defense
siehe auch
Cache Cleaner
Host Checker
Übersicht....74
Exchange Server, Unterstützung....110
externalAuthServerUnreachable, MIB-Objekt....197
externe Ports....123
Externer Port, Konfiguration....188

F

Fehlerbehebung
Richtlinienverfolgung....145, 378
Verwenden virtueller Sitzungen....379
Fehlermeldungen ändern....205
fileName MIB-Objekt....195
Firewall
anfordern....74
mit Cache Cleaner verwenden....91
Unterstützung....76
Freigabe
Definition in Ressourcenrichtlinien....333
FTP-Archiv, Definition....127

G

Gateway
für externen Port....187, 188
konfigurieren....187, 188
Gruppenmitgliedschaft, LDAP....262
Gültige Rollen, Definition....54, 57

H

Handheld-Geräte
aktivieren....183
Herunterfahren des IVE....359
Hilfe ändern....205
Hilfe, an Support wenden....ix
Hinweissymbole (Definition)....ix
Host Checker
API *siehe*
Host Checker, Clientschnittstelle
Host Checker, Server-Integrationsschnittstelle
ausführen....84, 90
auto-upgrade....207
Clientschnittstelle
aktivieren....75, 209
Übersicht....74
deinstallieren....85, 91
Einschränkungen angeben
Bereichsebene....81, 424
Ressourcenrichtlinienebene....61
Rollenebene....81, 424
Systemebene....206
Übersicht....76
Frequenzprüfung....206
Installationsprogramm
aktivieren....424
herunterladen....220
Übersicht....89
Verzeichnis....85, 91
Korrektur
konfigurieren....212, 215
Übersicht....78
Protokollierung deaktivieren....199
Richtlinien....76
Server-Integrationsschnittstelle
aktivieren....215
Übersicht....75
Übersicht....75
Verbindungssteuerungsrichtlinie....78, 207
Host, Definition in Ressourcenrichtlinien....305, 309
Hostname
Auflösung....125, 190
Definition in Ressourcenrichtlinien....305, 333, 334
maskieren....288

Hostüberprüfungsmethode, Definition ... 76
HP OpenView, Unterstützung ... 127

I

IMAP
  Mailserver ... 354
  Unterstützung ... 106, 107, 110
Import
  schnell ... 139
  Standard ... 139
  vollständig ... 139
Importmodi
  Standard ... 139
  vollständig ... 139
Importmodus ... 369
  Schnellimport ... 369
  Standardimport ... 369
  Vollständiger Import ... 369
Info (Protokollmeldung), Definition ... 128
InfoExpress
  erzwingen ... 208
  Integration ... 76
Installation
  Kontaktaufnahme mit Support, Hilfe ... ix
Installationsprogramme, herunterladen ... 362
Instant Virtual Extranet
  siehe IVE
interne Ports ... 123
Interner Port, Konfiguration ... 123, 187
Internet Explorer
  JVM-Ausführung ... 72
  siehe Internet Explorer
Internet Explorer, JVM ausführen ... 72
Internet Mail Application Protocol, Unterstützung ... 106
IP-Adresse
  Anmeldeeinschränkungen, Benutzer ... 418, 425
  Auflösung ... 125, 190
  Benutzeranforderungen angeben ... 46
  Definition in Ressourcenrichtlinien . 305, 310, 333, 334
  Einschränkungen ... 418, 419, 421, 422, 423, 425
  für externen Port ... 187, 188
  konfigurieren ... 187, 188
  Network Connect, Zuordnung ... 97
IPEntry MIB-Objekt ... 196
ipEntry MIB-Objekt ... 196
ipIndex MIB-Objekt ... 196
IP-Quelladresseinschränkungen konfigurieren ... 39, 40, 46
ipValue MIB-Objekt ... 196
IVE
  CASQUE-Authentifizierung ... 239
  Definition ... 33
  Erstkonfiguration ... 37
  in LAN (Abbildung) ... 34
  Kennwortoptionen ... 225
  Kennwortverwaltung ... 225
  Konfiguration (grundlegende Schritte) ... 35
  RADIUS für Erkennung konfigurieren ... 244
iveAppletHits MIB-Objekt ... 196
iveConcurrentUsers MIB-Objekt ... 196
iveCpuUtil MIB-Objekt ... 195
iveDiskFull MIB-Objekt ... 198
iveDiskNearlyFull MIB-Objekt ... 198
iveFileHits MIB-Objekt ... 196
iveLogFull, MIB-Objekt ... 197
iveLogNearlyFull, MIB-Objekt ... 197
iveMaxConcurrentUsersSignedIn, MIB-Objekt ... 197
iveMemoryUtil MIB-Objekt ... 195
iveNCHits MIB-Objekt ... 196
iveReboot, MIB-Objekt ... 197
iveRestart MIB-Objekt ... 198
iveSAMHits MIB-Objekt ... 196
iveShutdown, MIB-Objekt ... 197
iveStart, MIB-Objekt ... 197
iveSwapUtil MIB-Objekt ... 196
ivetermHits MIB-Objekt ... 196
iveTooManyFailedLoginAttempts, MIB-Objekt ... 197
iveTotalHits MIB-Objekt ... 196
iveWebHits MIB-Objekt ... 196

J

J.E.D.I.
  siehe Endpunktsicherheit – Übersicht
Java Virtual Machine
  siehe JVM
Java-Applet
  siehe Applet
Java-Applets
  Verbindungen angeben ... 316, 318, 319
Java-Plug-In, Cache ... 73
JavaSoft-Zertifikat ... 72
Juniper Endpoint Defense Initiative
  siehe Endpoint Defense
Juniper Installer Service, Beschreibung ... 362
Juniper Networks Support ... ix
JVM
  Applet-Signierung ... 72
  mit nicht unterstützten Versionen arbeiten ... 118

K

Kanonisches Format
  Übersicht ... 305, 309, 333, 341, 344
Kennwörter
  Klartext ... 135
  neue Benutzer ... 136
  verschlüsselt ... 135
  XML-Datei ... 135
Kennwortverwaltung
  konfigurieren ... 230
Konfiguration, Systemaktualisierung ... ix
Konfigurationsdatei
  ACLs und Lesezeichen exportieren ... 366
  ACLs und Lesezeichen importieren ... 369
  lokale Benutzerkonten exportieren ... 365
  lokale Benutzerkonten importieren ... 365
  System exportieren ... 364
  System, importieren ... 364

Konsole
Administrator
siehe Webkonsole
seriell
siehe Serielle Konsole
Konventionen (Definition)
Symbole ix
Text ix
Korrektur
konfigurieren 212, 215
Übersicht 78
Kundensupport x

L

LAN, Netzwerkeinstellungen ändern 187, 188
LDAP-Server
siehe Authentifizierungsserver, LDAP
leeres Tag
XML 134
Lesezeichen
Datei erstellen 293, 294
exportieren 366
für das Web erstellen 284, 285, 293, 295, 296, 298
für SSH erstellen 296
für Telnet erstellen 296
importieren 369
Option aktivieren 290
Lizenzen
Aktualisierung 162
erstellen 160
Übersicht 158
logDescription MIB-Objekt 197
logFullPercent, MIB-Objekt 195
logID MIB-Objekt 196
logMessageTrap MIB-Objekt 198
logName MIB-Objekt 196
logType MIB-Objekt 197
Lokaler Authentifizierungsserver
Siehe Authentifizierungsserver, lokale Authentifizierung
Lokaler IVE-Server
Siehe Authentifizierungsserver, lokale Authentifizierung 225
löschen
Konfiguration 140
Lotus Notes
Unterstützung 106, 110

M

Mail
Server konfigurieren 354
Spitzennutzungsstatistik 199
Major (Protokollmeldung), Definition 127
Malwareerkennung, Anforderungen angeben 75
Management Information Base, Übersicht 127
MAPI, Unterstützung 106, 108
Maskieren von Kennwörtern in Compact HTML 185
Maximale Übertragungseinheit, Konfiguration 188, 189
McAfee
erzwingen 208
Integration 76
meetingCount MIB-Objekt 196
meetingHits MIB-Objekt 196
meetingLimit MIB-Objekt 198
meetingUserCount MIB-Objekt 195
meetingUserLimit MIB-Objekt 198
memUtilNotify MIB-Objekt 198
Methode, Hostüberprüfung 76
MIB, Übersicht 127
Microsoft Authenticode-Zertifikat 72
Microsoft JVM*Siehe* JVM
Minor (Protokollmeldung), Definition 127
Mobile HMTL-Seiten
aktivieren 184
MS Exchange
Protokoll, Unterstützung 106
Unterstützung 108
MTU, Konfiguration 188, 189

N

Namenssperrung, Unterstützung 235
Namespaces
XML 136
Netscape
JVM-Ausführung 73
Mail, Unterstützung 109
Messenger, Unterstützung 107
Network Connect
Abbildung 98
Optionen festlegen 299
Ressourcenrichtlinien 344
Rollen 57
Übersicht 38, 46, 95
Verwendung 96
Network Time Protocol verwenden 155
Netzmaske
Benutzeranforderungen definieren 46
Definition in Ressourcenrichtlinien 310
für externen Port 187, 188
konfigurieren 187, 188
Netzwerk
Einstellungen
erstmalig 123, 186
konfigurieren 123, 187, 395
Hostnamen für lokale Auflösung angeben 190
Pakete, Sniffing 382
statische Routen angeben 124, 189
Netzwerkeinstellungen exportieren 366
Neubooten des IVE 359
Neuschreiben
Durchgangsproxy 117, 321
Neustarten des IVE 359
New PIN-Modus, Unterstützung 234
Next Token-Modus, Unterstützung 234
NHC-Integration
siehe Host Checker-API
Nslookup-Befehl 383, 384

NT-Domäne
Siehe Authentifizierungsserver, Active Directory
NTML, Konfiguration 223
NTP verwenden 155
Nullserver
Siehe Authentifizierungsserver, anonymer Server

O

Optimiertes NCP aktivieren 182
Optionen für das Teilen von Tunneln 299
Oracle, Unterstützung 118
Outlook Express, Unterstützung 106
Outlook, Unterstützung 106, 108, 109
OWA, Unterstützung 110

P

PassGo Defender RADIUS-Server, Konfiguration 239
password
Anmeldungen einschränken
user 422
Sicherheitsanforderungen festlegen 49
Permissive Zusammenführung
Übersicht 58
Persönliche Firewall
mit Cache Cleaner verwenden 91
siehe Firewall
Unterstützung 76
Pfad
Definition in Ressourcenrichtlinien 310, 333, 334
Ping-Befehl 383, 384, 395
PKI, Definition 65
Plattform aktualisieren 360
Policy Tracing (Unterregisterkarte) 145
POP
Clients 109
Mailserver 354
Unterstützung 106, 107, 110
Port
Anforderungen
konfigurieren 209
Übersicht 74, 77
extern, ändern 187, 188
Ports
Definition in Ressourcenrichtlinien 310
extern 123
intern 123
Post Office Protocol
siehe POP
Pragma No-Cache (PNC, Header) 314
Privater Schlüssel
importieren 167
productName, MIB-Objekt 195
productVersion, MIB-Objekt 195
Proprietäre Images, Anforderungen angeben 74
Protokoll, Definition in Ressourcenrichtlinien 305, 309
Protokollierung
Clientprotokolle
Cache Cleaner 91
deaktivieren 199
konfigurieren 191
Protokolldateien speichern 191
Richtlinienverfolgung 378
Schweregrade 127
zu protokollierende Ereignisse angeben 192
Proxy
siehe Durchgangsproxy
Prozessprüfung
konfigurieren 209
Übersicht 74, 77
Public Key Infrastructure, Definition 65

R

RADIUS
Siehe Authentifizierungsserver, RADIUS
referenzielle Integrität 137
Regel
Cachesteuerung 312
Definition 77
konfigurieren 60, 262
Regeln für die Zwischenspeicherung von Inhalten 312
Registerkarten
Routen 189
Registrierungseinstellungen
Prüfung
konfigurieren 211
Übersicht 74, 77
Reihenfolge
Elemente 137
Ressourcen, Bestandteil einer Ressourcenrichtlinie 59
Ressourcenrichtlinien
Auswertung 60
Codierung 339
Datei 332
Definition 35, 40
Durchgangsproxy 322
E-Mail-Client 354
exportieren 366
importieren 369
Java 316, 317, 319
konfigurieren 308, 341, 417
Network Connect 344
Selektives Neuschreiben 320
Server 305
Übersicht 59
UNIX/NFS-Dateien 334, 337
vorkonfigurierte Richtlinien 35
Web 308, 309
Windows-Dateien 333, 334
Zwischenspeicherung 312
Ressourcenrichtlinien für Zwischenspeicherung 312
Richtlinie
verfolgen 145, 378
Richtlinien
Anmelderichtlinien *Siehe* Anmelderichtlinien
Ressourcenrichtlinien *Siehe* Ressourcenrichtlinien
Richtlinien für Java-Zwischenspeicherung 316, 319

Rolle
Anmeldeeinschränkungen
Kennwort ... 422
über Host Checker-Richtlinie ... 423
über IP ... 418, 425
über Zertifikat ... 421
Auswertung ... 57
Benutzersitzungsoptionen festlegen ... 279
Bestandteil einer Ressourcenrichtlinie ... 59
Definition ... 35, 39, 56
Einschränkungen ... 278
Einstellungen verwalten ... 277
exportieren ... 366
importieren ... 369
konfigurieren ... 276, 417
Lesezeichen
Datei erstellen ... 293, 294
für das Web erstellen 284, 285, 293, 295, 296, 298
für SSH erstellen ... 296
für Telnet erstellen ... 296
Optionen verwalten ... 277
vordefinierte Rollen ... 35
Zugriffssteuerung für Webserver ... 311, 344, 347, 351
Zuordnung ... 39, 51, 53, 57, 261
Zusammenführung ... 58
Rollenbasierte Quell-IP-Aliase ... 57
Routes (Registerkarte) ... 189
RSA ACE/Server
Hostnamen auflösen ... 52
Siehe Authentifizierungsserver, ACE/Server

S

Schlüssel
privat, *Siehe* Privatschlüssel
Schnellimport ... 139
SCP, Systemsnapshot ... 396
sdconf.rec generieren ... 236
Selektives Neuschreiben ... 320
Serielle Konsole
für systembezogene Aufgaben verwenden 63, 153, 201, 255, 273, 303, 357, 389
Server
Definition in Ressourcenrichtlinien ... 333, 334
für Authentifizierung verwendete Typen ... 52
Ressourcenrichtlinien ... 305
siehe auch Authentifizierungsserver
Server Certificate (Registerkarte), Certificates (Menü) ... 166
Serverkatalog konfigurieren ... 263
Sicherheitsoptionen
konfigurieren ... 164
signedInWebUsers, MIB-Objekt ... 195
Simple Mail Transfer Protocol
siehe SMTP-Mailserver
Simulieren von Benutzersitzungen ... 379
Sitzung
Optionen festlegen ... 279
permanente, konfigurieren ... 280
Roaming konfigurieren ... 280
Warnung bei Zeitüberschreitung ... 280
Zeitüberschreitung, Leerlauf ... 279
Zeitüberschreitung, maximale Dauer ... 279
Sitzungen beenden ... 156
Sitzungsparameter konfigurieren ... 57
Sitzungsrolle, Definition ... 57
Sitzungszeitbegrenzungen
Auswirkung auf Cache Cleaner ... 91
konfigurieren ... 39
Smart Caching ... 313
SMTP-Mailserver
aktivieren ... 354
Unterstützung ... 106
Snapshot ... 396
Snapshotdatei (zum Debuggen) ... 382
SNMP
Einstellungen angeben ... 193
IVE als Agent überwachen ... 193
Unterstützung ... 127
Software
herunterladen ... 155
installieren ... 360
Sperrlisten-Verteilungspunkt
Erläuterung ... 69
Herunterladen von CRLs ... 177
siehe Sperrlisten-Verteilungspunkt
Spyware, Anforderungen angeben ... 75
SSH
Lesezeichen erstellen ... 296
SSH-Optionen angeben ... 298
SSL
zulässige Verschlüsselungsstärke ... 165
zulässige Version ... 164
Standardimport ... 139
Standardimport, Modus ... 139
Startseite
anpassen ... 281
Start-Tag
XML ... 134
statische Routen ... 189
Sun JVM
siehe JVM
Superadministrator-Konto erstellen ... 396
swapUtilNotify MIB-Objekt ... 198
Sygate
Enforcement API
erzwingen ... 208
integrieren ... 76
Security Agent
erzwingen ... 208
integrieren ... 76
Symbole (Definition), Hinweis ... ix
Syslog-Server konfigurieren ... 193
System
Daten archivieren ... 376
Debugging ... 381, 382, 383, 384
Konfiguration ... 359
Konfiguration exportieren ... 364
Konfiguration importieren ... 364
Software installieren ... 360
Statistik anzeigen ... 199

Systemdaten....359
Systemeigene Hostprüfung
siehe Host Checker

T

TCP-Dumpdatei (zum Debuggen)....382
Telnet
Lesezeichen erstellen....296
Telnetoptionen angeben....298
Temporäre Dateien entfernen....75, 87
Textkonventionen (Definition)....ix
TLS
zulässige Version....164
Traceroute-Befehl....383, 384, 395
Traps
Definition....127
konfigurieren....194
Tunnel für den Zugriff vor der Authentifizierung
Beschreibung....82
festlegen....216

U

Überprüfung....141
Übertragungsrate
konfigurieren....187, 188
Uhrzeit und Datum einstellen....155
UNIX/NFS-Datei
Ressourcenrichtlinien....337
UNIX/NFS-Dateien
Ressourcenrichtlinien
Definition....334
UNIX-Ressource
Lesezeichen....294
Unterstützung
kompatibel mit....381, 384
Unterstützung untergeordneter ACE/Server....235
URL
Zugriffsstatistik....199
user
'Benutzeradministratoren'
authentifizieren....223
Definition....229
Advanced Preferences (Seite)....290
Anmeldeeinschränkungen
Kennwort....422
über Browser....419
über Zertifikat....421
Attribute konfigurieren....261
Beenden erzwingen....156
Daten
exportieren....366
importieren....369
erstellen....227
Höchstanzahl....260
Konten
erstellen....227, 301
exportieren....365
importieren....365
verwalten....228
Kontoverwaltung....228
Rolle
Definition....56
Überwachung....156
USER (Variable)
in UNIX-Lesezeichen....294
in Web-Lesezeichen....284
in Windows-Lesezeichen....293

V

Verbindung testen....359
Verbindungssteuerungsrichtlinie, als
Host Checker-Option auswählen....78, 207
Vermittlung
Selektives Neuschreiben....321
Verschlüsselung
Beschreibung....34
Kennwörter....135
Stärke....165
Verzeichnisserver
siehe auch Authentifizierungsserver
Definition....53
Virensignaturen, Alter prüfen....211
virtuell
Hostname
konfigurieren....186
Umgebungen, Anforderungen angeben....75
Virtuelle Benutzersitzungen, aktivieren....379
Virtueller Hostname
konfigurieren....323
vollständiger Import....139
vollständiger Import, Modus....139
VPN ohne Client, Übersicht....95

W

Web
Lesezeichen erstellen....284, 285, 293, 295, 296, 298
Navigationsprobleme....381
Proxy angeben....329
Ressourcenrichtlinien....308, 309
Serverzugriffssteuerung....311, 344, 347, 351
Spitzennutzungsstatistik....199
Zugriffssteuerung....311, 344, 347, 351
Webkonsole
Beschreibung....37
Windows
Anmeldeinformationen....335
Windows Internet Naming Service-Server, Konfiguration 187
Windows, Unterstützung
Zertifikate....72
Windows-Datei
Ressourcenrichtlinien....334
Windows-Dateien
Ressourcenrichtlinien....333
Windows-Ressource
Lesezeichen....293
WINS
für externen Port....187, 188
Server, Konfiguration....187

X

XML
- Kennwörter ... 135
- Namespaces ... 136

XML importieren/exportieren
- Anmeldeseiten ... 367
- Benutzerrollen ... 368
- Bereiche ... 367
- delegierte Administratorrollen ... 368
- Elementreihenfolge ... 137
- Ende-Tag ... 134
- Importmodus ... 369
- Instanzdatei ... 133
- Instanzelemente ... 133
- leeres Tag ... 134
- lokale Benutzerkonten ... 368
- Netzwerkeinstellungen ... 366
- referenzielle Integrität ... 137
- Start-Tag ... 134
- Verarbeitungsanweisung ... 134
- XML-Instanz zu Benutzeroberfläche zuordnen ... 138

XML-Attribute ... 136
XML-Codebeispiel ... 134
XML-Instanzdatei
- überprüfen ... 141

Z

Zeitbegrenzungen
- *Siehe* Sitzungszeitbegrenzungen

Zeitüberschreitung
- Leerlaufzeit, Sitzung ... 279
- maximale Sitzung ... 279
- Warnung festlegen ... 280

Zertifikat
- Anmeldungen einschränken
  - user ... 421
- Appletzertifikat
  - Definition ... 65
  - importieren ... 181
- Attribute konfigurieren ... 261
- clientseitiges Zertifikat
  - Definition ... 65
- Codesignaturzertifikat
  - *siehe* Zertifikat, Appletzertifikat
- CRLs
  - aktivieren ... 177
  - Anzeigen von Details ... 174
- Einschränkungen konfigurieren ... 39, 40
- Hierarchie
  - Definition ... 67
  - Erläuterung ... 66, 68
- JavaSoft ... 72
- MS Authenticode ... 72
- Schlüssel
  - vorhandenen importieren ... 167
- selbst signiert ... 66
- Server
  - Definition ... 67
  - *siehe* Authentifizierungsserver, Zertifikatserver
- Serverzertifikat
  - Definition ... 65
  - erneuertes Zertifikat importieren ... 168
  - vorhandenen importieren ... 167
  - Zertifikatssignaturanforderung erstellen ... 169
  - Zertifikatssignaturanforderung importieren ... 170
- Sicherheitsanforderungen festlegen ... 48
- Signaturanforderung
  - erstellen ... 169
  - importieren ... 170
  - Zertifikat importieren ... 170
- Sperrliste ... 35
  - Definition ... 68
  - Erläuterung ... 69
- Sperrung
  - Definition ... 68
- unterstützte Formate ... 166, 171, 180
- Zertifizierungsstellenzertifikat
  - Aktivieren der CRL-Prüfung ... 177
  - Anzeigen von Details ... 181
  - Definition ... 65
  - erneuern ... 174
  - hochladen auf das IVE ... 171
  - Überprüfung ... 179

Zertifikatsperrliste
- *siehe* Zertifikat, Sperrliste

Zertifikatssignaturanforderung
- erstellen ... 169
- importieren ... 170
- Zertifikat importieren ... 170

Zertifizierungsstellenzertifikat
- *siehe* Zertifikat, Zertifizierungsstellenzertifikat

Zone Labs
- erzwingen ... 208
- integrieren ... 76

Zugriffssteuerung
- Liste (ACL)
  - exportieren ... 366
  - importieren ... 369
- Webressourcen ... 311, 344, 347, 351

Zugriffstunnel
- *Siehe* Tunnel für den Zugriff vor der Authentifizierung

Zugriffsverwaltung
- Einschränkungen festlegen ... 278

Zulässige Rollen, Definition ... 54

Juniper your Net™

www.juniper.net

CORPORATE HEADQUARTERS
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone 408 745 2000 or 888 JUNIPER
Fax 408 745 2100

Juniper Networks, Inc. has sales offices worldwide.

For contact information, refer to www.juniper.net.

Printed on recycled paper
50A051605